db-direct internet
Customer Self Administration

Version 11.1

User Guide

Table of Contents

Table of Contents 2

1 Overview 3

2 Detailed description 4

2.1 Installation 4
2.2 Product Scope 5

3 User Front-End 6

3.1 db-direct internet home page 6
3.2 Administration of Users 8
3.2.1 Quick Links 8
3.2.2 User Details 9
3.2.3 Maintain User Roles 21
3.2.4 Maintain Joint Category Limits 29
3.2.5 Maintain Sign-On Passwords 31
3.3 Active User Reports 32
3.4 Audit Reports 33

4 Table of Figures 35

1 Overview

Deutsche Bank's db-direct internet ('dbdi') is the leading global electronic banking system in the market today. It provides a single, multi-lingual platform for both Corporates and Financial Institutions to access the Bank's Cash Management, Custody and Trade Finance services from anywhere in the world via the Web.

The Customer Self Administration ("CSA") module provides db-direct internet customers the option to maintain (viewing, creating, updating, locking and deleting) user IDs and user profiles.

Additionally, user passwords to logon to db-direct internet can be created for new users as well as logon passwords can be reset for existing users.

Self administration functions will be performed by your designated Customer Self Administrators. Involvement of Deutsche Bank staff will only be required for the setup of IDs for Customer Self Administrators, respectively their user profiles and access rights and registration of Authorized Persons (Signatories on the accounts) for certain countries. These procedures are detailed in the following sections.

The current self administration module is not covering the administration of domain settings, products, company details and accounts. Those items will be maintained by Deutsche Bank, please contact your Implementation & Services Manager or Account Management contact.

2 Detailed description

2.1 Installation

User profiles of Customer Self Administrators will be created and maintained by Deutsche Bank staff upon your request and will be documented in annexes to the db-direct internet legal agreement.

Legal documentation is required to be returned to Deutsche Bank duly signed on behalf of the customer before the administration can take place.

The Customer Self Administration ("CSA") module will give db-direct internet customers the opportunity to create, modify, lock and delete user profiles and user roles, i.e. defining viewing rights for account information and viewing, editing, verification and authorization rights & limits for transaction orders as well. In addition, User Administrators can issue new or reset existing user logon passwords for their domain without the involvement of Deutsche Bank staff.

Please note: For certain countries for accounts with Deutsche Bank, authorization rights must be covered by signatory rights, which have been agreed locally on account level (account mandate, board resolutions). In this case, the CSA module will perform a Signatory Validation. For detailing the countries, please contact your Implementation & Services Manager or Account Management counterpart.

Designated Customer Self Administrators will be able to use the CSA module. Customer Self Administrators will be selected by the customer and identified by name, address, email, telephone, fax, etc. Customer Self Administrators will be documented in annexes of the legal documentation and will be administered by Deutsche Bank staff. For each of them a copy of an ID document (ID card, passport) needs to be provided.

A designated Customer Self Administrator will need, for security reasons, to sign and return a Receipt Form to acknowledge their designation as Customer Self Administrator and, if they are a new User, also to confirm that they have changed their initial password.

2.2 Product Scope

The customer can choose to define what administration tasks the Customer Self Administrator can / will take on:

- User Maintenance: view, edit (includes creation, update and deletion), suspend or unlock and approve (control) of user details, IDs and user rights.

  User rights include normal user rights in the sense of view, edit (includes creation, update and deletion) and pre-verifying of account information and transaction orders as well as defining of authorization rights and limits for releasing transactions.

  Note, that for certain countries Deutsche Bank is obliged to validate authorizers (approvers) and their authorization (approver) rights against signatory rights agreed locally (as per account mandate, board resolutions).

  User rights, that can be maintained, do not include CSA administration rights, as only the Bank can maintain CSA administration rights.

- Create and Reset Log-on Passwords for User ID's: creation and reset of log-on passwords for User IDs.

- Public Keys (electronic signature) will be active within 15 minutes after uploading to db-direct internet server.
  The key generation protocol needs to be provided to your Customer Self Administrator.

For added security, each action performed requires an approval (control) by a second Administrator (dual control).

Each action (setup, update and delete operations; approvals) performed by a Customer Self Administrator will be documented and recorded. Active and audit trail reports can be generated and downloaded at any time by designated Customer Self Administrators. Audit data will be stored by Deutsche Bank for 10 years.

3 User Front-End

3.1 db-direct internet home page

The CSA functions can be accessed via the db-direct internet home page clicking the “Maintain Users” menu. After clicking, a new browser session will be opened for the CSA module.

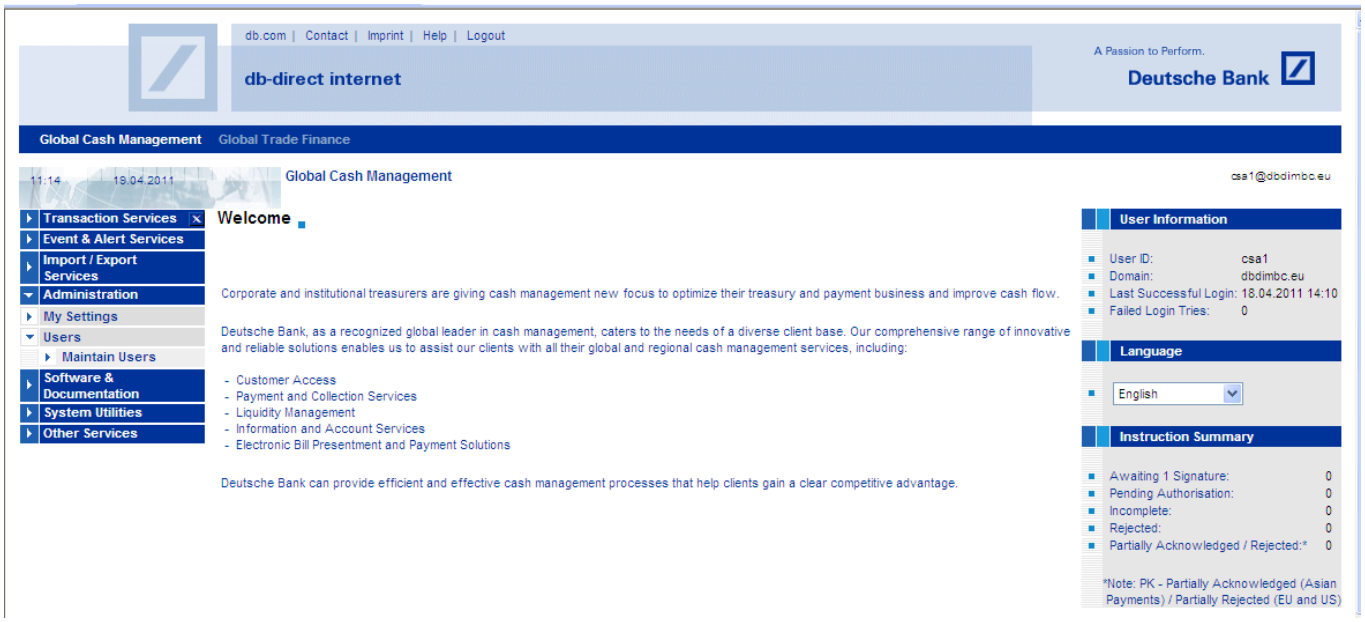

db.com | Contact | Imprint | Help | Logout
db-direct internet
A Passion to Perform.
Deutsche Bank
Global Cash Management
Global Trade Finance
Global Cash Management
csa1@dbdimbc.eu
Transaction Services
Event & Alert Services
Import / Export Services
Administration
My Settings
Users
Maintain Users
Software & Documentation
System Utilities
Other Services
Welcome
Corporate and institutional treasurers are giving cash management new focus to optimize their treasury and payment business and improve cash flow.
Deutsche Bank, as a recognized global leader in cash management, caters to the needs of a diverse client base. Our comprehensive range of innovative and reliable solutions enables us to assist our clients with all their global and regional cash management services, including:
- Customer Access
- Payment and Collection Services
- Liquidity Management
- Information and Account Services
- Electronic Bill Presentment and Payment Solutions
Deutsche Bank can provide efficient and effective cash management processes that help clients gain a clear competitive advantage.
User Information
User ID: csa1
Domain: dbdimbc.eu
Last Successful Login: 18.04.2011 14:10
Failed Login Tries: 0
Language
English
Instruction Summary
Awaiting 1 Signature: 0
Pending Authorisation: 0
Incomplete: 0
Rejected: 0
Partially Acknowledged / Rejected:* 0
*Note: PK - Partially Acknowledged (Asian Payments) / Partially Rejected (EU and US)
db.com | English | Logout
db-direct
A Passion to Perform.
Deutsche Bank
Entitlement Admin
Welcome Antje Beheerder
Your last login session was 27.05.2011 01:07:41 PM
You are administering: dbdimbc.eu
My Settings
Persons
User Details
Quick Links
User Details
User Roles
Joint Category Limits
Sign On Passwords
Reports
Quick Links
Welcome to the Administration module of db-direct
Maintain User
User Name
--Please Select--
VIEW USER PERMISSIONS
ADD USER
Maintain User Role
User Role Name
--Please Select--
ADD ENTITLEMENT ROLE
ADD AUTHORIZATION ROLE
Records pending for approval:
Users: -
Entitlement Roles : 1
Authorization Roles: -
Joint Categories: -
Sign On Passwords: -
Records locked due to signatory permission failure:
Users -

Figure 1: Access the CSA module from the main menu of the dbdi homepage

The functions available to the Customer Self Administrator depend on the administration tasks (CSA user profile) defined in the legal agreement (annex 1.3.4).

Here is an overview of the available CSA functions:

CSA menu:

Quick Links: Allows the Customer Self Administrator to navigate quickly and directly to unapproved items. Facilitates to quickly inquire and setup users and user roles.

User Details: Provides an overview of the existing users. Allows the Customer Self Administrator to create and/or update users as well as assigning of user roles to users.

User Roles: Allows the Customer Self Administrator to maintain access rights, authorization limits and privileges, which can be assigned to users via 'User Details'.

Joint Category Limits: Allows the Customer Self Administrator to maintain joint authorization requirements.

Sign On Passwords: Allows the Customer Self Administrator to create and reset dbdi logon passwords.

Reports: Allows the Customer Self Administrator to generate active and audit reports for users, user roles and at joint category level.

3.2 Administration of Users

3.2.1 Quick Links

The Quick Links screen allows the Customer Self Administrator to quickly view and access unapproved users, user roles, authorization limits and joint limit categories, see right hand table.

Facilitates to quickly inquire and setup users and user roles.

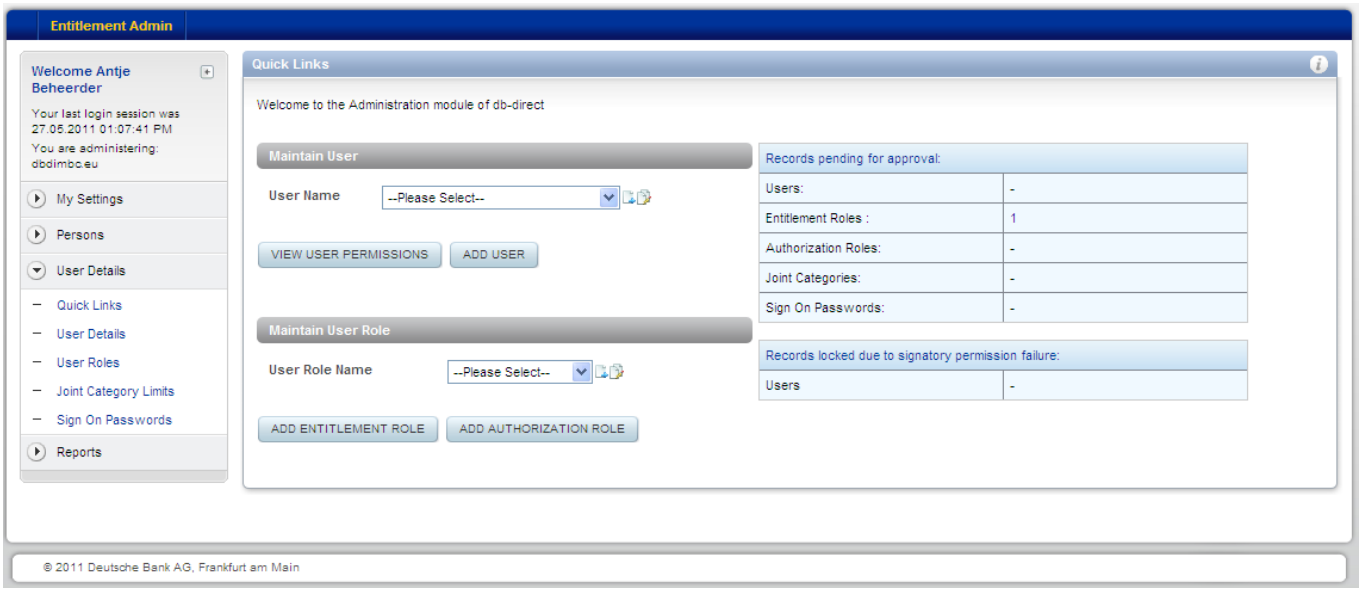


Figure 2: Quick Links screen

3.2.2 User Details

This screen allows the Customer Self Administrator to view, edit (includes creation, update and deletion), suspend or unlock users and approve (control) any user changes.

3.2.2.1 User Summary

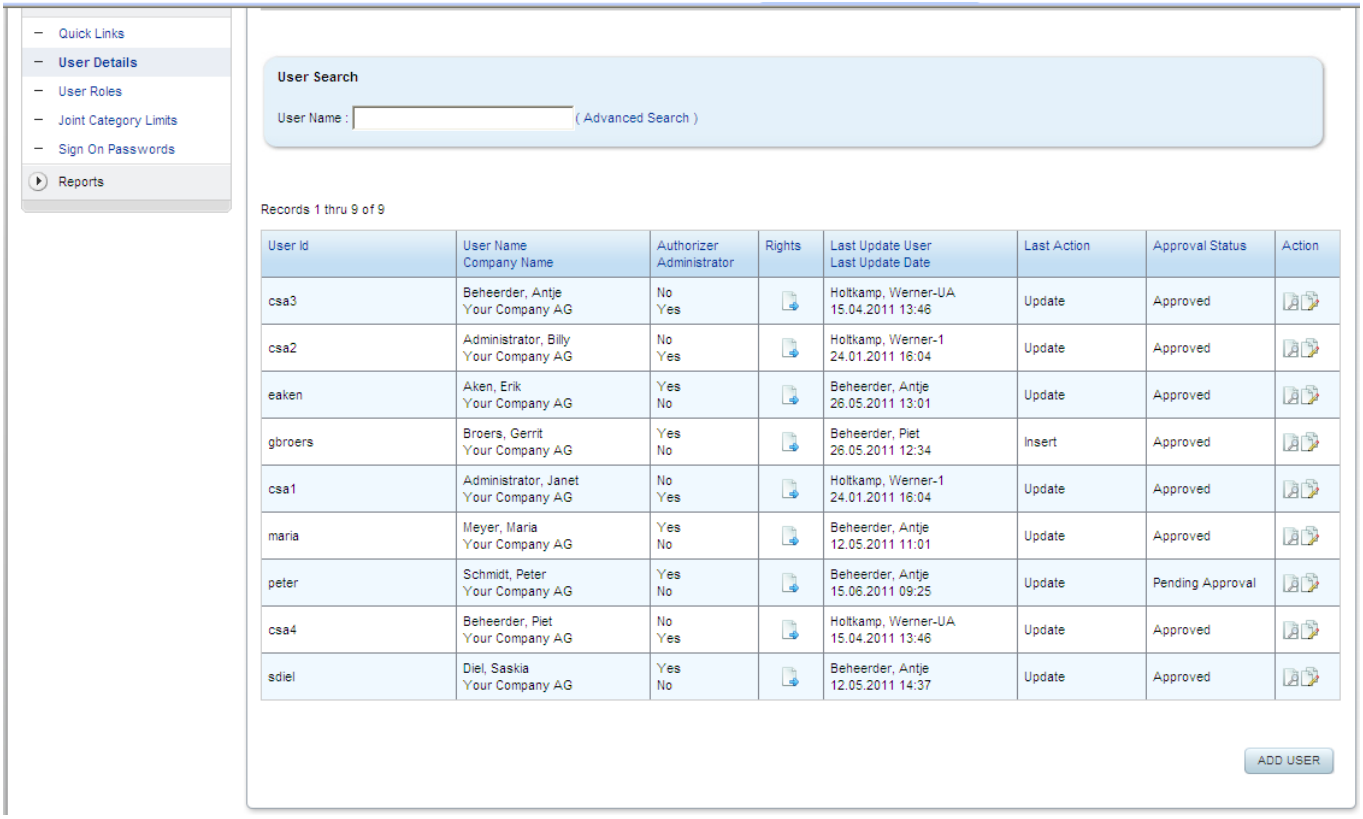

Quick Links
User Details
User Roles
Joint Category Limits
Sign On Passwords
Reports
User Search
User Name :
(Advanced Search)
Records 1 thru 9 of 9
User Id
User Name
Company Name
Authorizer
Administrator
Rights
Last Update User
Last Update Date
Last Action
Approval Status
Action
csa3 Beheerder, Antje Your Company AG No Yes Holtkamp, Werner-UA 15.04.2011 13:46 Update Approved
csa2 Administrator, Billy Your Company AG No Yes Holtkamp, Werner-1 24.01.2011 16:04 Update Approved
eaken Aken, Erik Your Company AG Yes No Beheerder, Antje 26.05.2011 13:01 Update Approved
gbroers Broers, Gerrit Your Company AG Yes No Beheerder, Piet 26.05.2011 12:34 Insert Approved
csa1 Administrator, Janet Your Company AG No Yes Holtkamp, Werner-1 24.01.2011 16:04 Update Approved
maria Meyer, Maria Your Company AG Yes No Beheerder, Antje 12.05.2011 11:01 Update Approved
peter Schmidt, Peter Your Company AG Yes No Beheerder, Antje 15.06.2011 09:25 Update Pending Approval
csa4 Beheerder, Piet Your Company AG No Yes Holtkamp, Werner-UA 15.04.2011 13:46 Update Approved
sdiel Diel, Saskia Your Company AG Yes No Beheerder, Antje 12.05.2011 14:37 Update Approved
ADD USER

Figure 3: User summary from the User Details menu

Above summary screen will be shown when clicking the Users menu. A summary list of existing users will be displayed.

For viewing user details press the magnifying glass icon , for editing and approving of data press the pencil icon , for adding a new user press the 'Add User' button.

Please note:

1) Each administration requires the approval of a second Customer Self Administrator (dual control requirement), those items are indicated as 'Pending Approval' (see column Approval Status of above screen shot).
   For performing the approval, the second administrator would need to invoke the user by clicking the pencil icon and after reviewing the user details, in case of updates by clicking 'Pending Changes', could apply Approve, otherwise Rollback.

Figure 4: Buttons displayed in case an object is "Pending Approval"

2) In case an object (here a User) has been updated by Deutsche Bank (system updates), the Last Update User of such an object will be indicated as “CAAA, Import Approval” (see screen shot below)

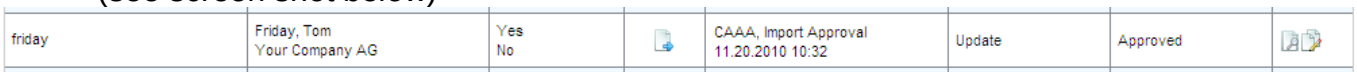


Figure 5: Objects with Last Update User as "CAAA, Import Approval"

3.2.2.2 Add / Edit Users and User Details

For creating a User, please click the ‘Add User’ button either in the Quicklinks screen (see lower screen of figure 1) or the ‘Add User’ button at the bottom of the User Summary screen (see figure 3).

For updating an existing User, please click the pencil icon of that particular user in the Action column of the User Summary screen (see figure 3):

General User Details are displayed in the first tab, further details on the Person level will be shown by clicking the link ‘View Person Details’ (see figure 6).

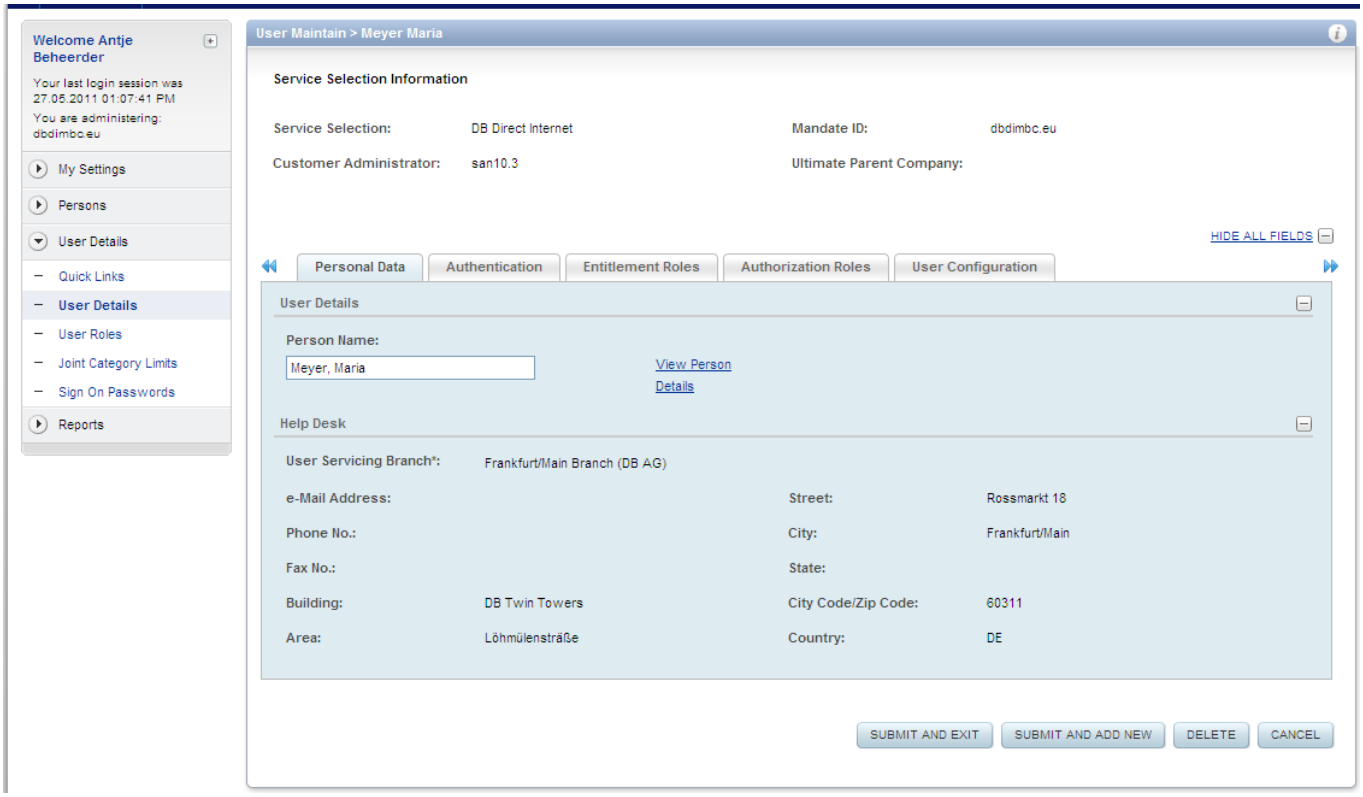


Figure 6: Personal Data tab of User Details

This is the Personal Data screen of the Maintain Person screen.
Note, that the WebSSO (web single sign on) User ID is generally the email ID of the person

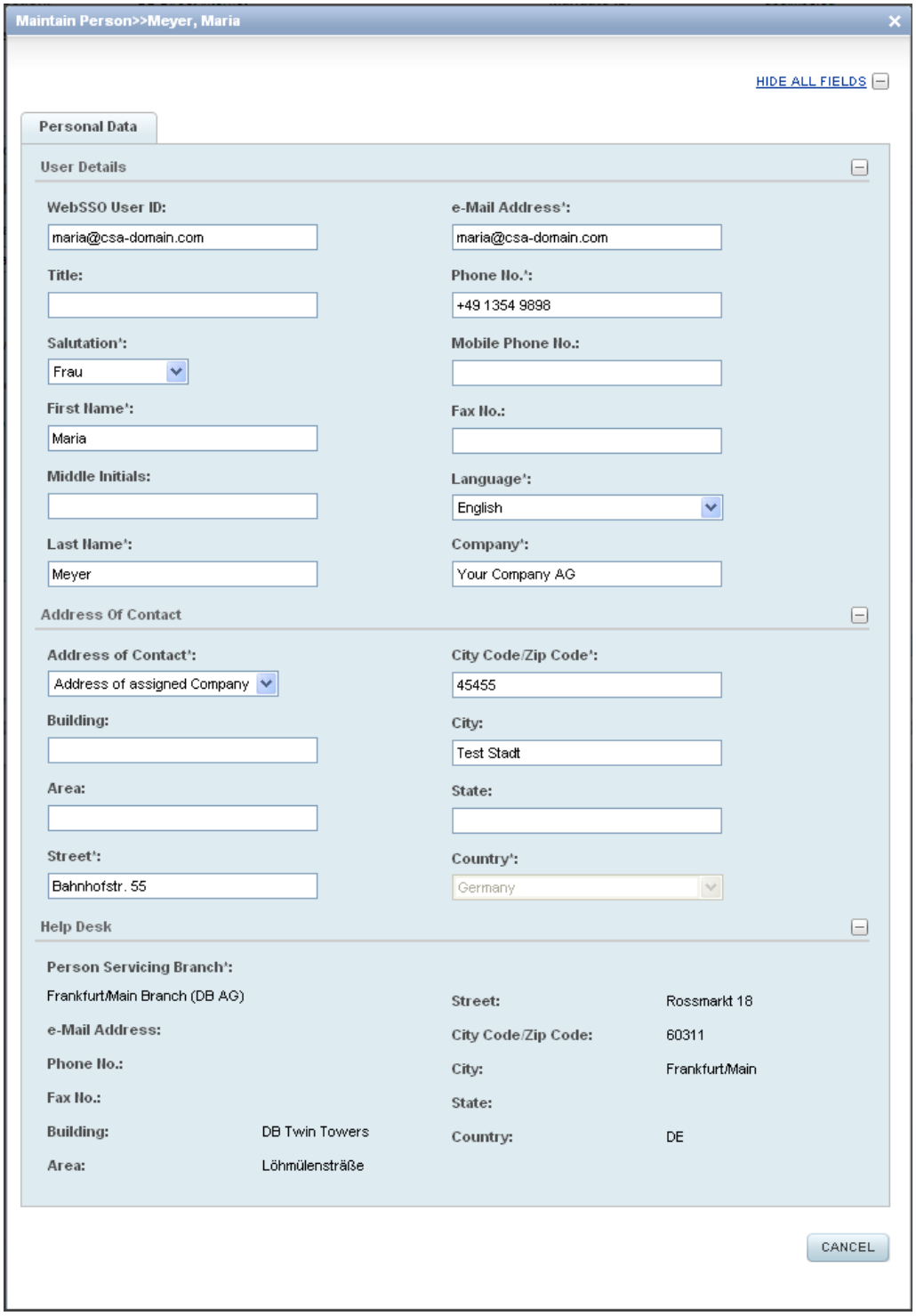


Figure 7: Personal Data screen accessed via User Details

For updating Person details, once existing, click Maintain Person and click the edit icon in the Action column:

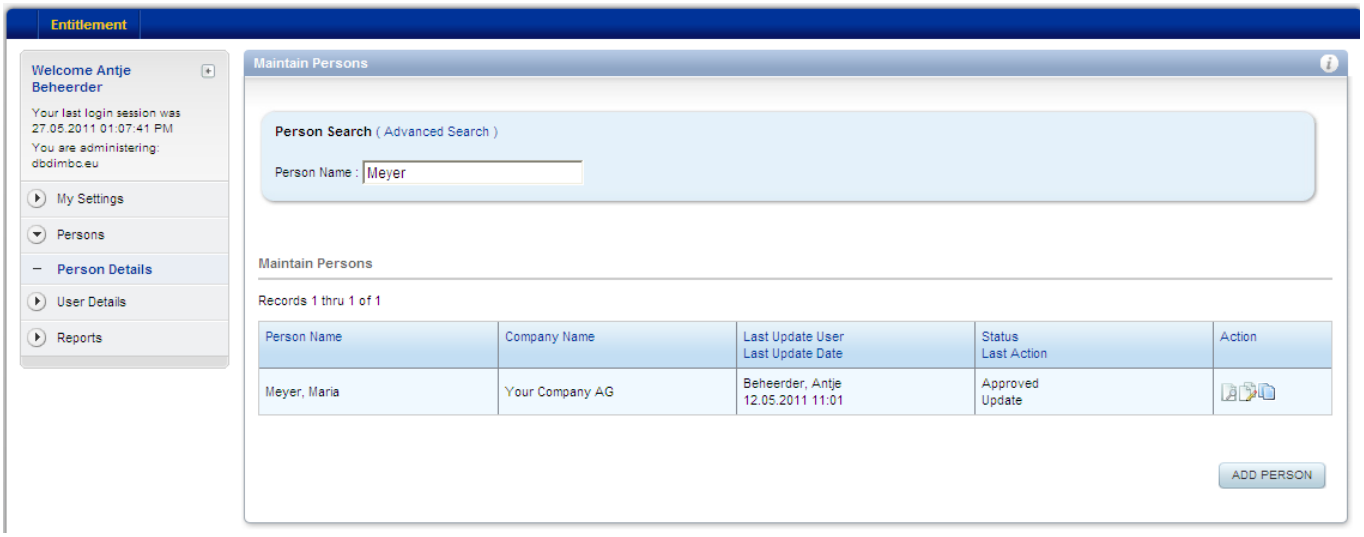


Figure 8: Maintain Person summary

Changes applied on Person level will be updating the details on User level.

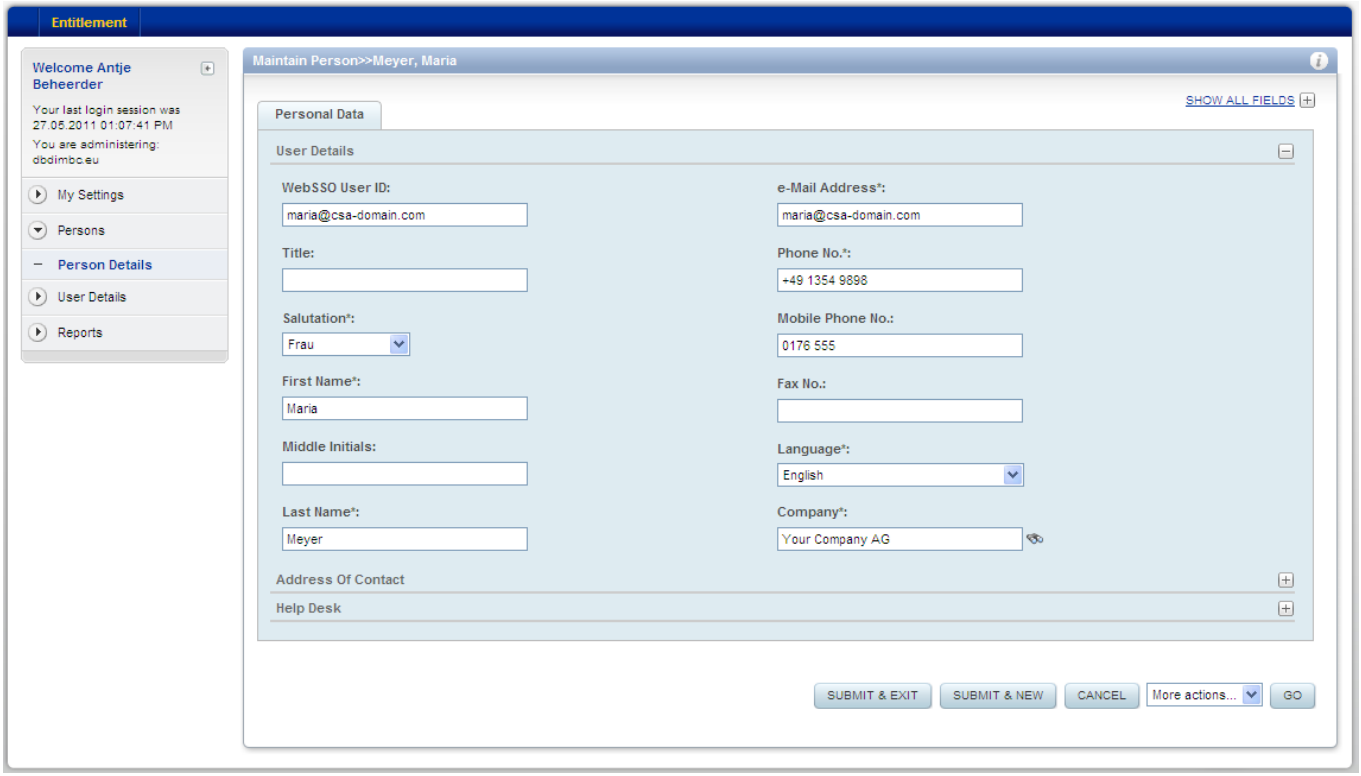


Figure 9: Personal Data tab of Maintain Person

User details related to authentication like user ID, login mode and accessibility information can be updated in the Authentication tab.

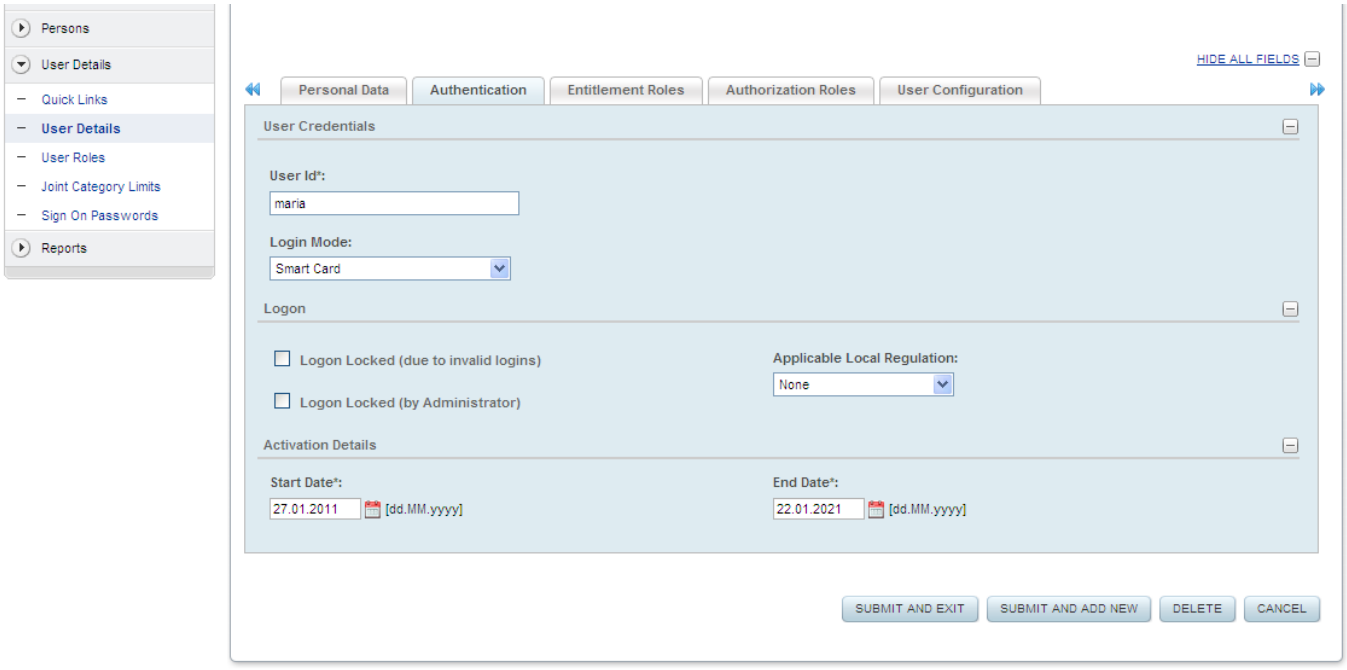


Figure 10: Authentication tab of the Maintain User screen

The User ID normally consists of the first name or last name of the user, but cannot exceed 16 characters.

3.2.2.3 Assigning Entitlement Roles

In the Entitlement Rights screen, the Customer Self Administrator can assign entitlement roles (setup of those user roles will be explained below) by moving the selected roles from the Available Roles box to the Selected Roles box (reassigning vice versa).

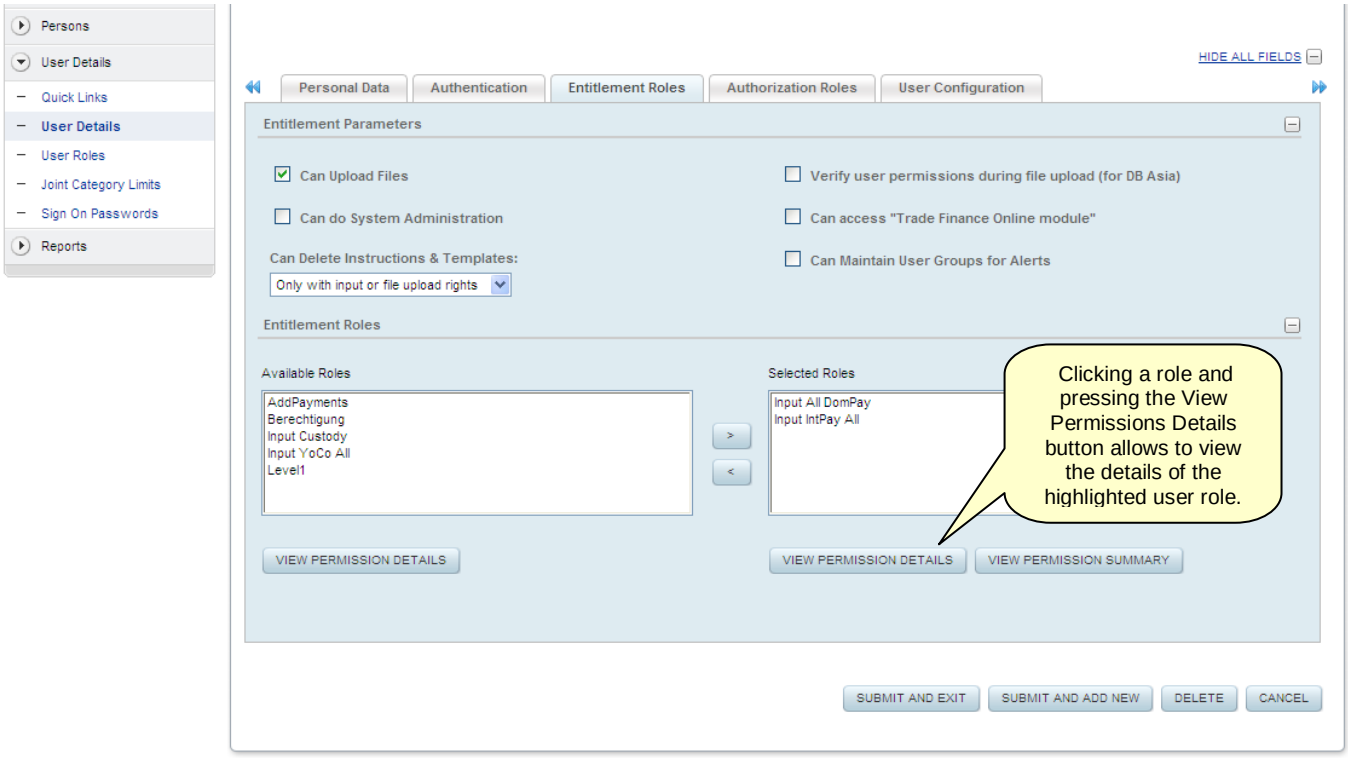


Figure 11: Entitlement Rights tab of the Maintain User screen

Pressing the “View Permissions Details” button allows viewing the details of the highlighted user role.

Tick the ‘Can Upload File’ box to activate that this user can upload files.

Tick the ‘Verify user role view permissions during file upload’ box to activate xxx

3.2.2.4 Assigning Authorization Roles

The Authorization Rights screen allows the Customer Self Administrator to assign authorization roles (setup of those user roles will be explained below) by moving the selected roles from the Available Roles box to the Selected Role box (reassigning vice versa).
Note, the 2 arrow buttons for moving the user roles will only be shown in case the 'Allowed to Authorise Instructions' box has been ticked.

After an Authorization Role has been assigned to a user, a validation will be performed after the submit has been clicked in order to ensure that those Authorization Rights are covered by Signatory Rights as specified in the Company Mandate (only applicable for certain DB account locations, you might want to check with your Implementation Manager).

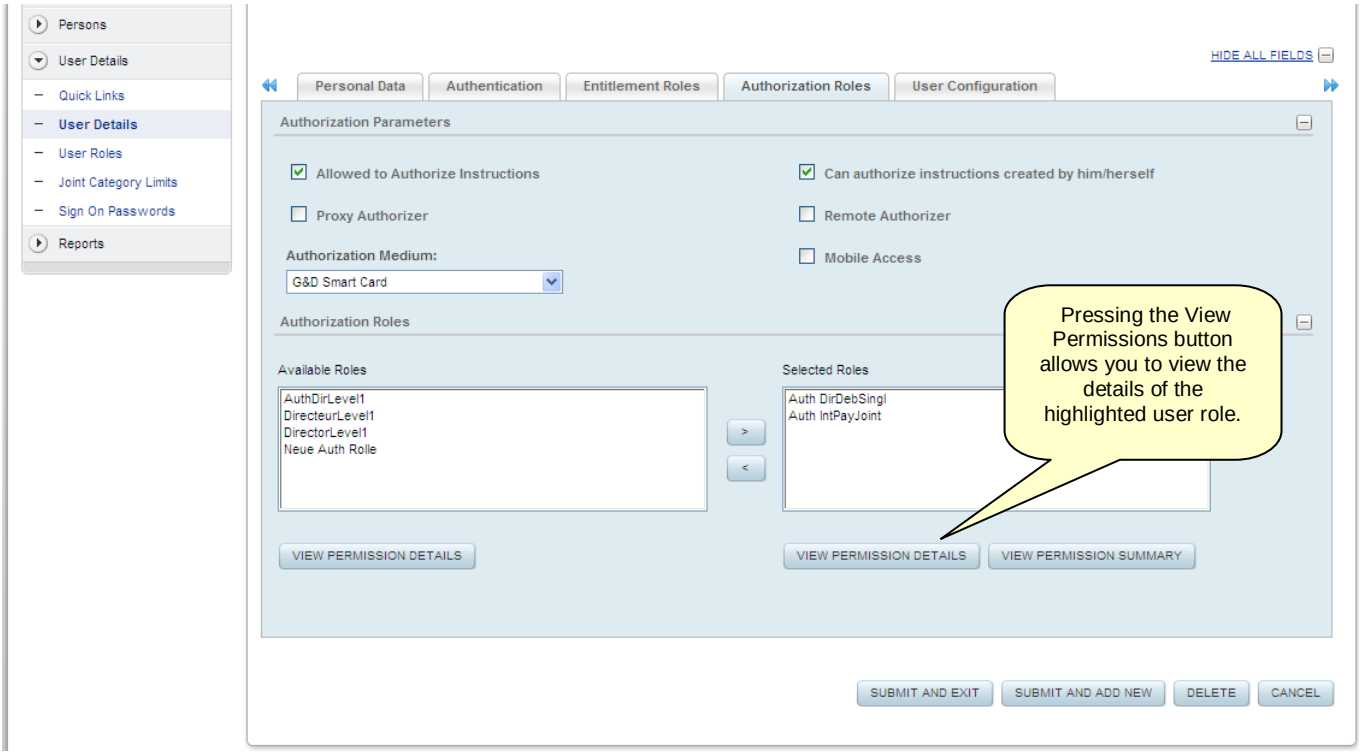


Figure 12: Authorization Rights tab Maintain Users screen

Please note:

1. User Roles indicated with 'Signatory Role', if existing, represent the available Signatory Rights (as per signatory card, account mandate) for countries where Deutsche Bank is obliged to validate authorization (channel) rights. This role is not editable for Customer Self Administrators.
2. Pressing the "View Permissions Details" button allows viewing the details of the highlighted user role.

3.2.2.5 Maintaining User Configurations

In the User Configuration screen, the Customer Self Administrator can define further user settings:

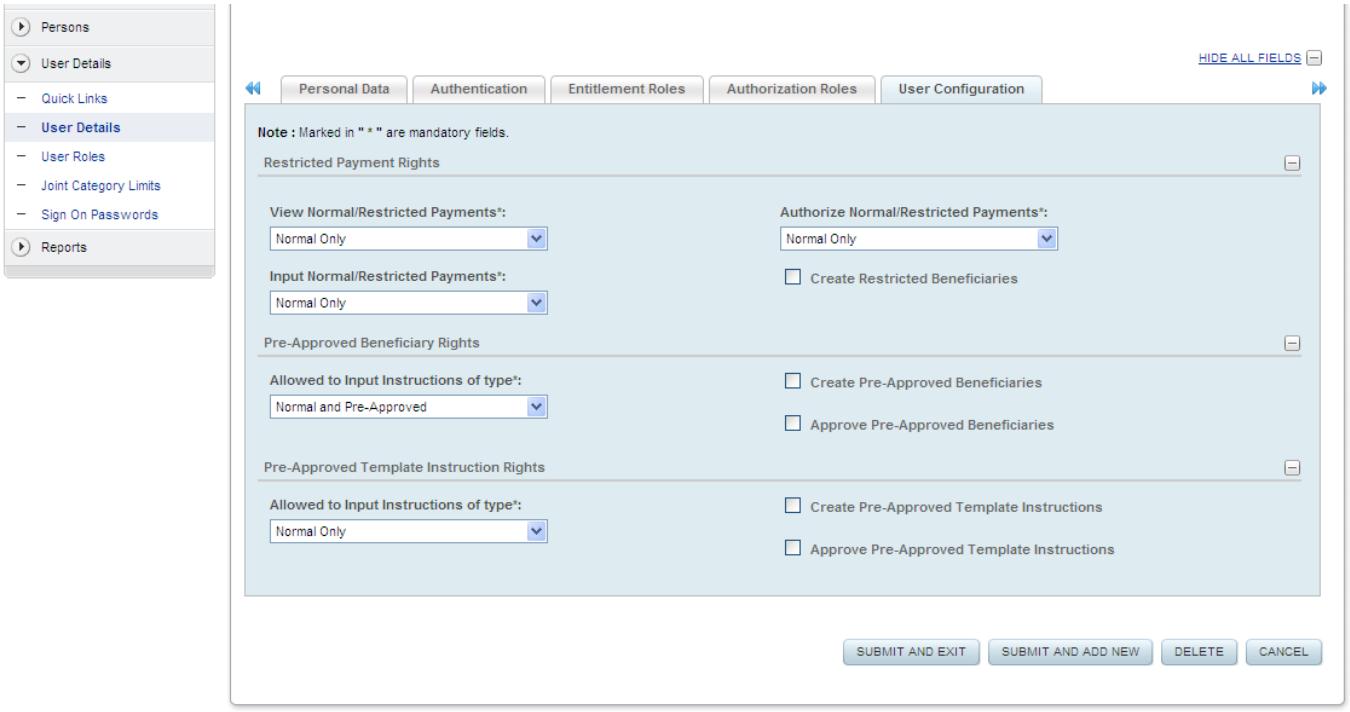


Figure 13: User Configuration of the Maintain User screen

<u>Restricted Payment Rights section:</u>
Defines whether the User may View, Input or Authorize Normal or Restricted Payments.
Can define whether Normal, Restricted or Both.
Option to create Restricted Beneficiaries.

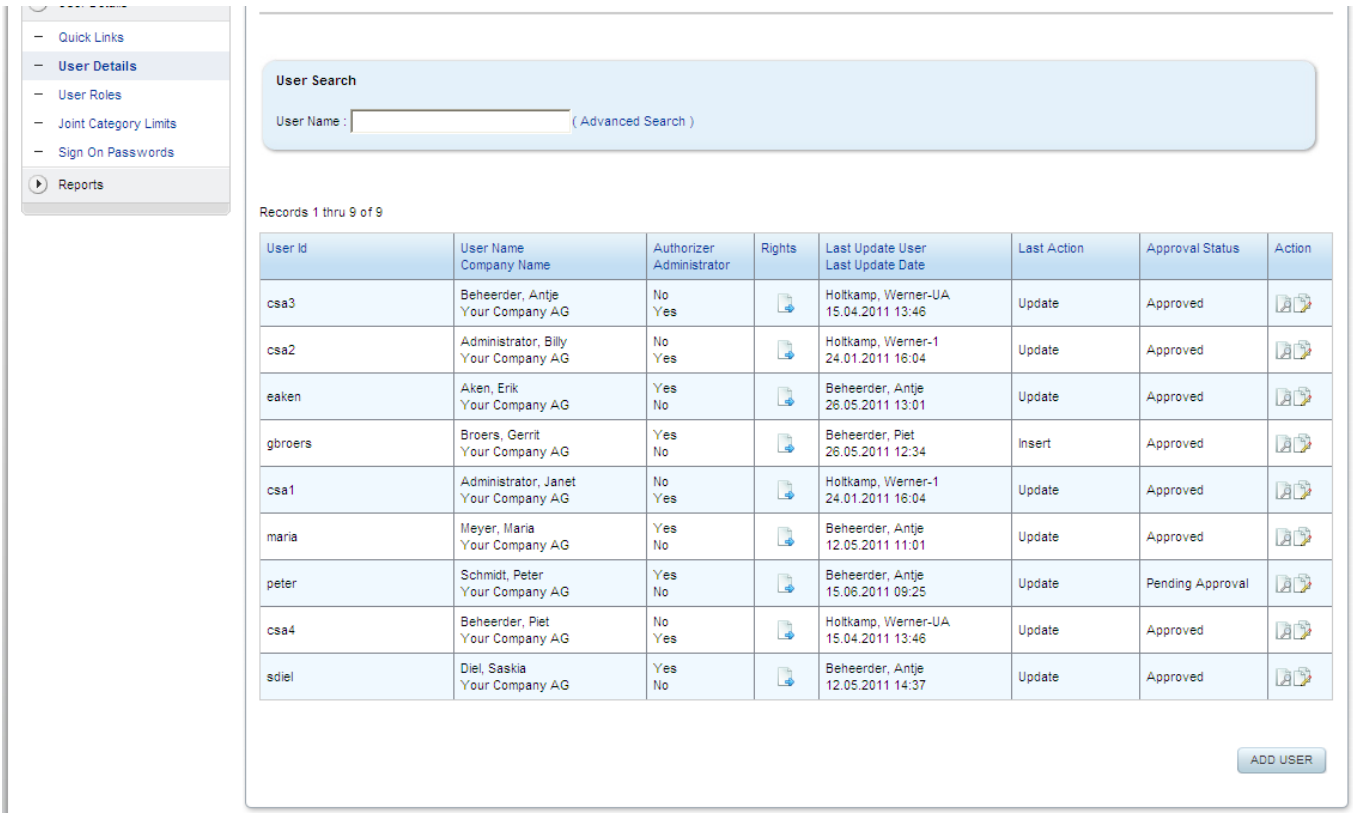
<u>Pre-Approved Beneficiary Rights section:</u>
Defines whether the User may Input any payments relating to Normal, Pre-Approved or Both.
Defines whether the User may create or approve Pre-Approved Beneficiaries.

<u>Pre-Approved Template Instruction Rights section:</u>
Defines whether the User may Input using Normal Templates, Pre-Approved Templates or Both.
Defines whether the User may create or approve Pre-Approved Template Instructions.

3.2.2.6 Approving User Details

Each operation is subject to an approval to be performed by a second Customer Self Administrator (dual control). The change will only be active after an approval.

In below example, the user with User ID ‘peter’ is in Pending Approval status:



User Id	User Name Company Name	Authorizer Administrator	Rights	Last Update User Last Update Date	Last Action	Approval Status	Action
csa3	Beheerder, Antje Your Company AG	No Yes		Holtkamp, Werner-UA 15.04.2011 13:46	Update	Approved	
csa2	Administrator, Billy Your Company AG	No Yes		Holtkamp, Werner-1 24.01.2011 16:04	Update	Approved	
eaken	Aken, Erik Your Company AG	Yes No		Beheerder, Antje 26.05.2011 13:01	Update	Approved	
gbroers	Broers, Gerrit Your Company AG	Yes No		Beheerder, Piet 26.05.2011 12:34	Insert	Approved	
csa1	Administrator, Janet Your Company AG	No Yes		Holtkamp, Werner-1 24.01.2011 16:04	Update	Approved	
maria	Meyer, Maria Your Company AG	Yes No		Beheerder, Antje 12.05.2011 11:01	Update	Approved	
peter	Schmidt, Peter Your Company AG	Yes No		Beheerder, Antje 15.06.2011 09:25	Update	Pending Approval	
csa4	Beheerder, Piet Your Company AG	No Yes		Holtkamp, Werner-UA 15.04.2011 13:46	Update	Approved	
sdiel	Diel, Saskia Your Company AG	Yes No		Beheerder, Antje 12.05.2011 14:37	Update	Approved	

Figure 14: Summary from the User Details menu, where one user records are in ‘pending approval’ status

A second Customer Self Administrator needs to invoke the record (pressing the pencil icon) and can choose to Approve or Rollback it (there will be respective buttons in the bottom of the screen).

In order to inquire pending changes, please click the respective button ‘Pending Changes’:

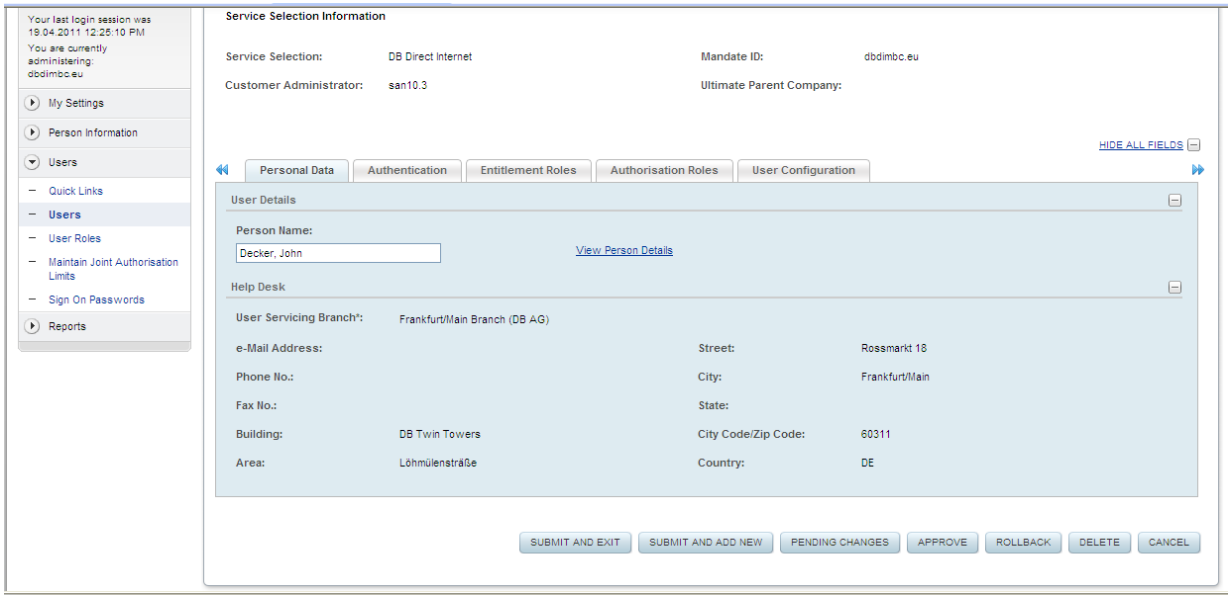


Figure 15: Approve & Rollback button

3.2.2.7 User 'Locked'

In case, a user has been locked, this will be indicated in the Authentication tab.

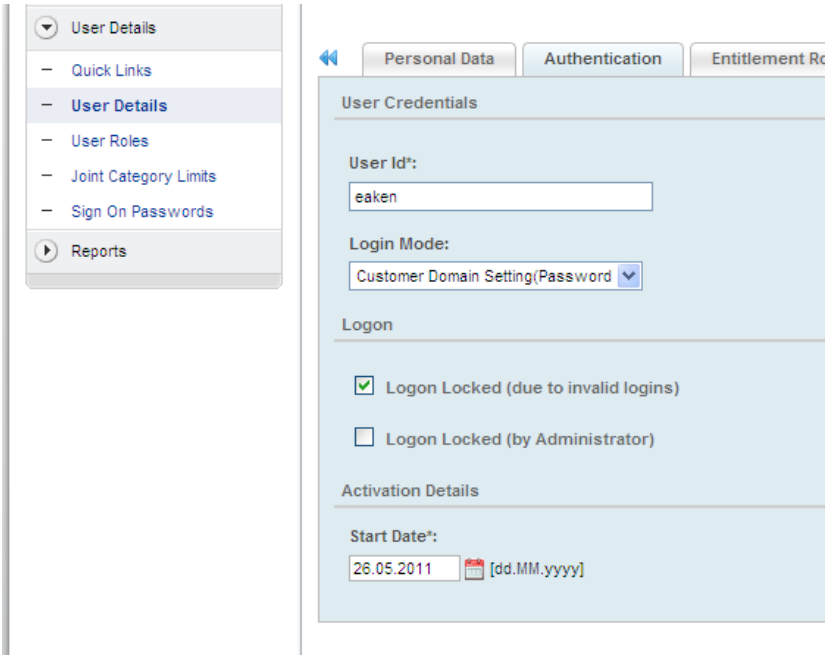


Figure 16: User Lock flags

There are 2 lock options:

The upper option will be enabled by the application in case the logon to the application was failing 3 times due to key error. The user would be able to reset the password by answering the prompted questions after clicking 'Forgot Password?' from the logon screen (soft lock):

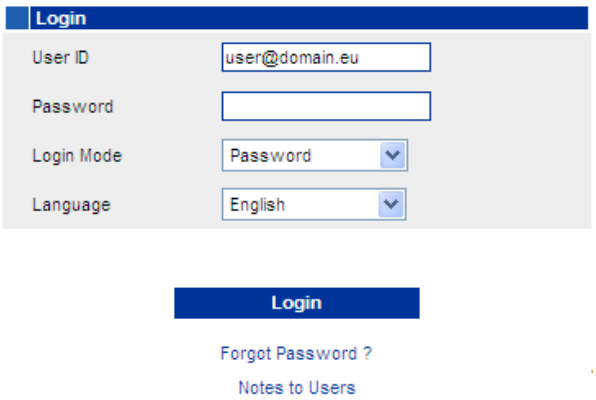


Figure 17: User Self Password reset via dbdi logon screen

Otherwise, the user needs to be unlocked by the CSA admin and the password would need to be reset (see below).

In case the lower option has been ticked off the user will not be able logon (hard lock).

3.2.3 Maintain User Roles

Via the Maintain User Role function, the Customer Self Administrator can view, edit (includes creation, update and deletion) and approve (control) user roles.

User roles need to be assigned to users (see above 3.1.2.3 and 3.1.2.4).

The same user role can be assigned to more than one user; a user can be linked with more than one user roles.

There are two types of user rights:

- Entitlement rights
  Those rights deal with inquiry rights for account information, additionally viewing, editing and verification rights for transactions and performing system administration.

- Authorization rights
  Those rights concern the rights for authorizing of transaction orders.

The User Role summary screen is listing the existing user roles:

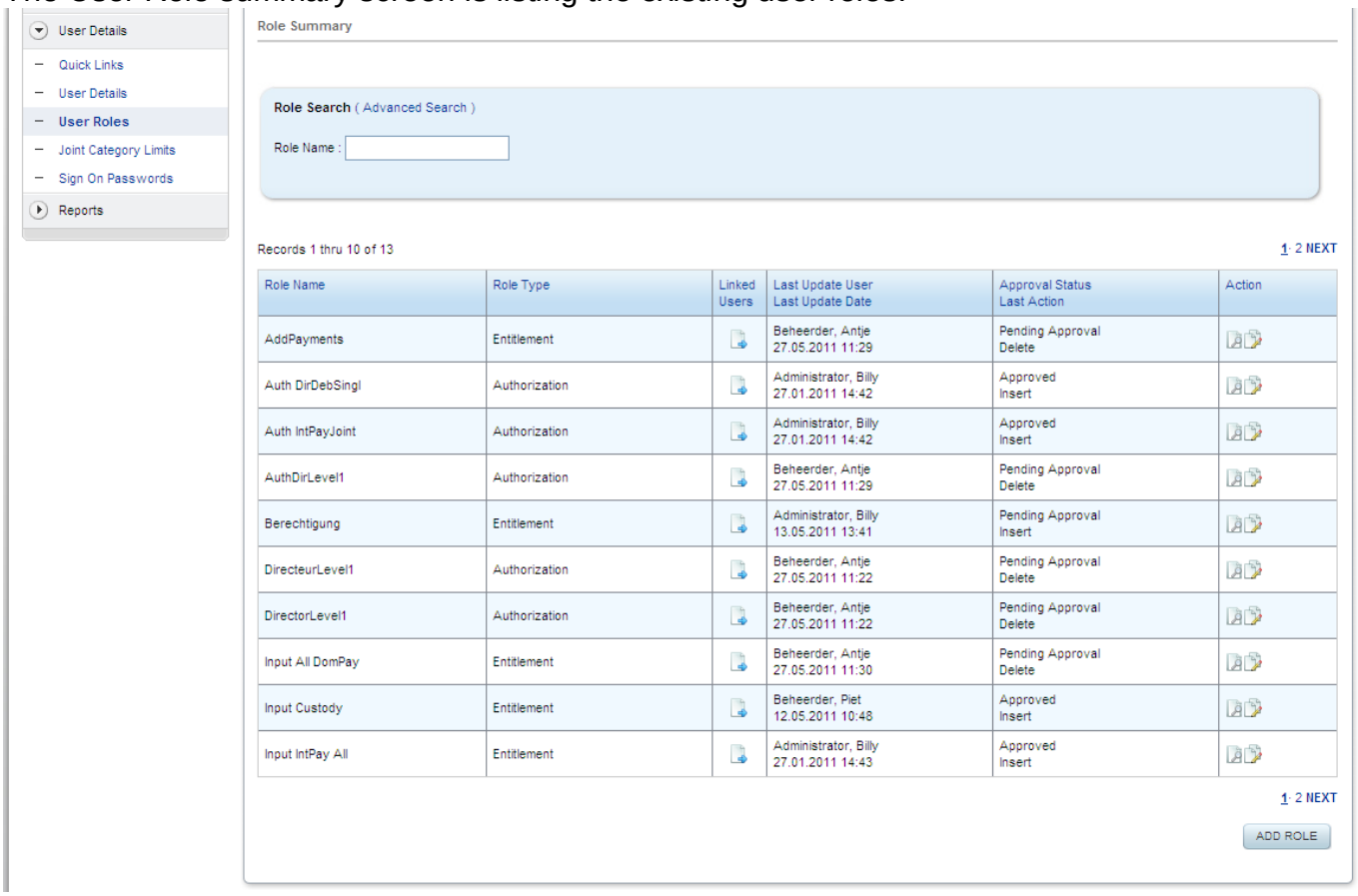


Figure 18: Summary screen of Maintain User Roles

For creating a new role, please click the “Add Role” button.
For amending an existing user role, please click the pencil icon in the Action column.

3.2.3.1 Maintain Entitlement Rights

Via this screen Entitlement Roles can be maintained. Inquiry, editing and pre-verification rights are considered Entitlement or 'Normal User' rights.

Below screen displays the existing permissions of user role 'View AI All'.

For example, line number 1 explains that for the certain account of company 'Your Company AG' Insert / Update / Delete permissions for Domestic Payments have been defined.

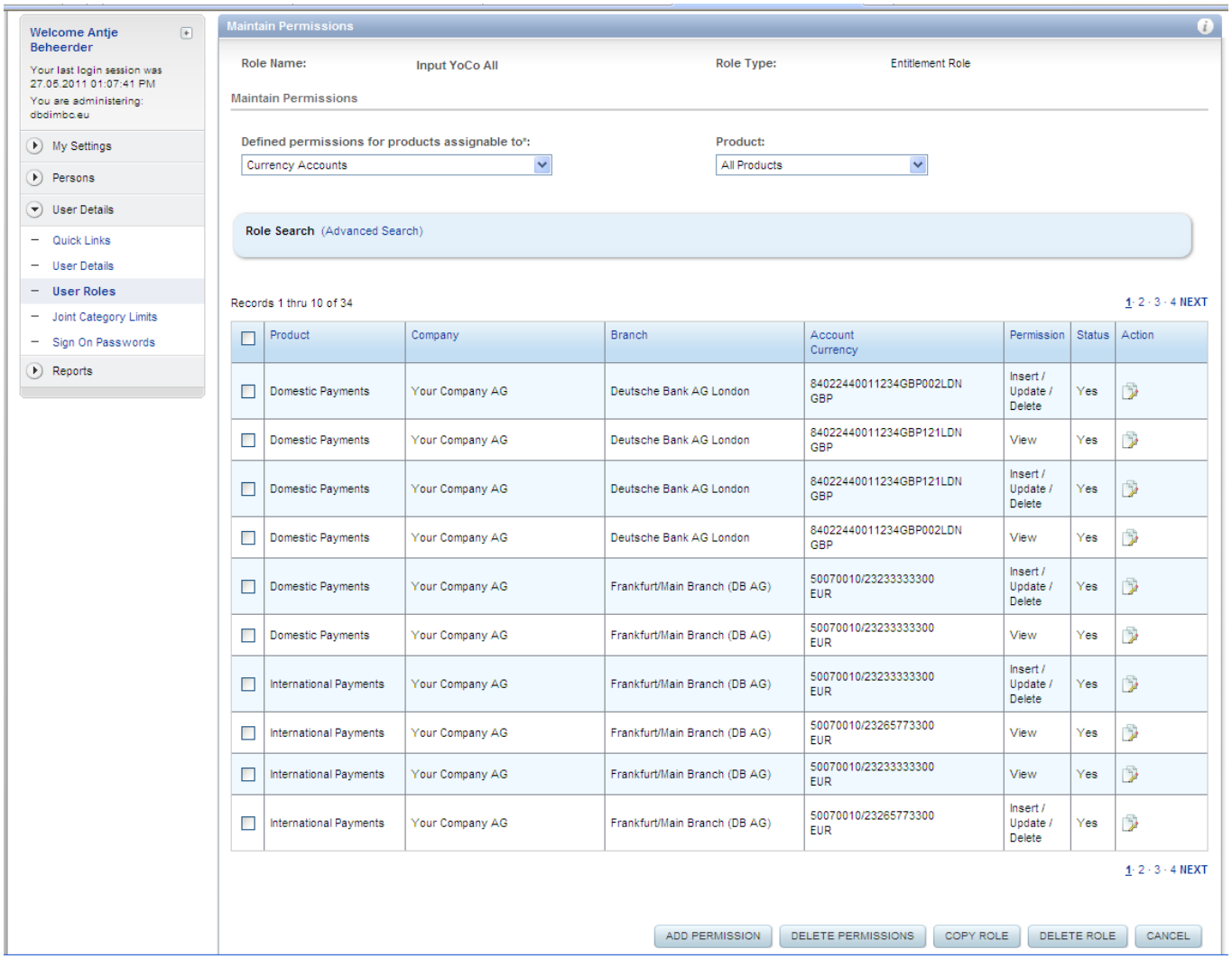
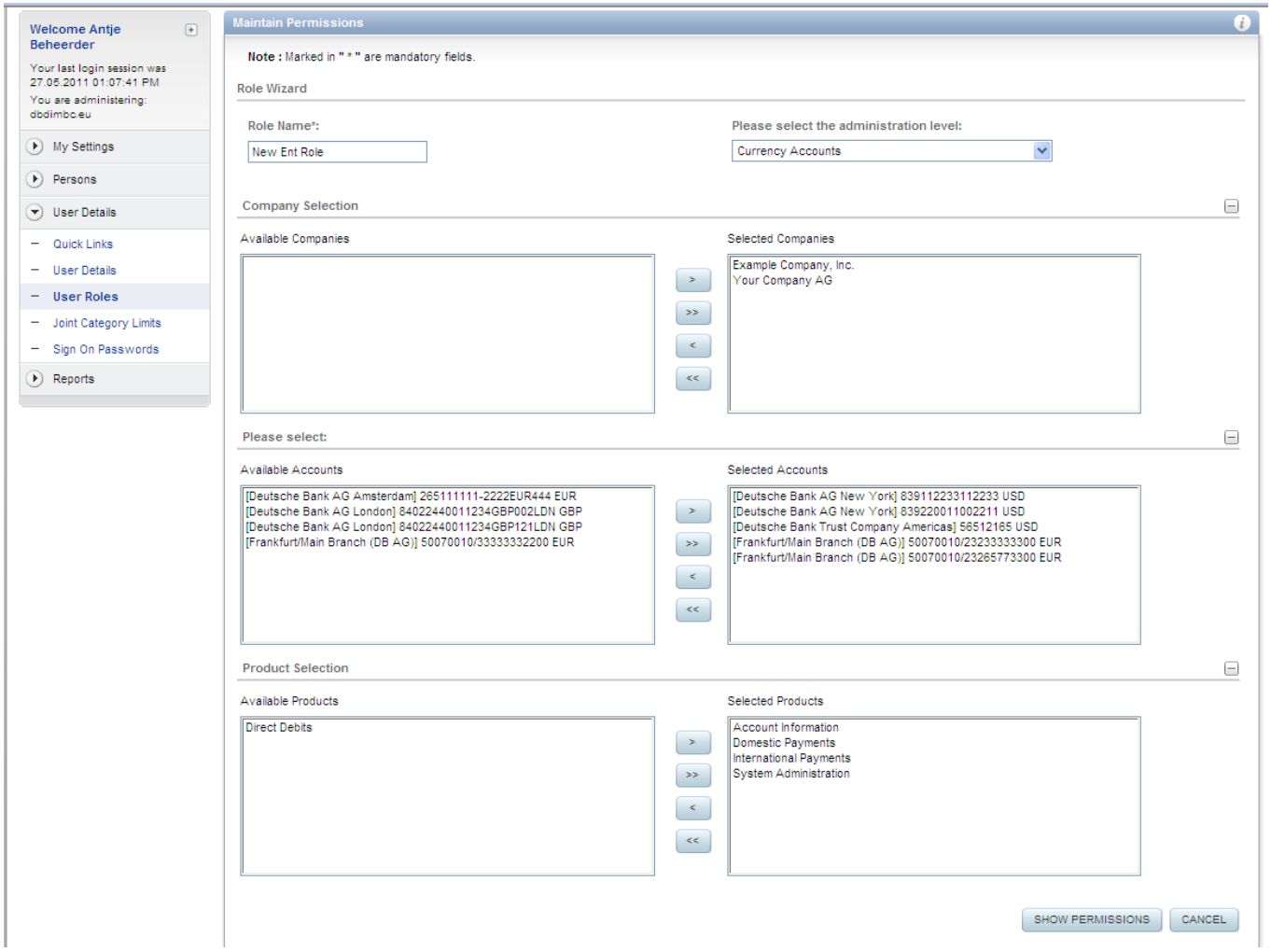

Welcome Antje Beheerder
Your last login session was 27.05.2011 01:07:41 PM
You are administering: dbdimbc.eu
My Settings
Persons
User Details
Quick Links
User Details
User Roles
Joint Category Limits
Sign On Passwords
Reports
Maintain Permissions
Role Name: Input YoCo All
Role Type: Entitlement Role
Maintain Permissions
Defined permissions for products assignable to*:
Currency Accounts
Product:
All Products
Role Search (Advanced Search)
Records 1 thru 10 of 34
1 · 2 · 3 · 4 NEXT
Product | Company | Branch | Account Currency | Permission | Status | Action
Domestic Payments | Your Company AG | Deutsche Bank AG London | 84022440011234GBP002LDN GBP | Insert / Update / Delete | Yes
Domestic Payments | Your Company AG | Deutsche Bank AG London | 84022440011234GBP121LDN GBP | View | Yes
Domestic Payments | Your Company AG | Deutsche Bank AG London | 84022440011234GBP121LDN GBP | Insert / Update / Delete | Yes
Domestic Payments | Your Company AG | Deutsche Bank AG London | 84022440011234GBP002LDN GBP | View | Yes
Domestic Payments | Your Company AG | Frankfurt/Main Branch (DB AG) | 50070010/23233333300 EUR | Insert / Update / Delete | Yes
Domestic Payments | Your Company AG | Frankfurt/Main Branch (DB AG) | 50070010/23233333300 EUR | View | Yes
International Payments | Your Company AG | Frankfurt/Main Branch (DB AG) | 50070010/23233333300 EUR | Insert / Update / Delete | Yes
International Payments | Your Company AG | Frankfurt/Main Branch (DB AG) | 50070010/23265773300 EUR | View | Yes
International Payments | Your Company AG | Frankfurt/Main Branch (DB AG) | 50070010/23233333300 EUR | View | Yes
International Payments | Your Company AG | Frankfurt/Main Branch (DB AG) | 50070010/23265773300 EUR | Insert / Update / Delete | Yes
1 · 2 · 3 · 4 NEXT
ADD PERMISSION
DELETE PERMISSIONS
COPY ROLE
DELETE ROLE
CANCEL

Figure 19: Permissions summary of Maintain Entitlement User Roles

Existing permissions can be removed by enabling the check box and pressing the "Delete Permissions" button, permissions can be amended by pressing the pencil icon in the Actions column.

Press the "Add Permission" button for applying new or further permissions.

The following Wizard (pop up window) will be displayed when adding a new Entitlement role by clicking the Add Role bottom either in the Quicklinks or User Role screens:



Hit 'Show Permissions':

Figure 20: Wizard screen of Maintain Entitlement User Roles

Administration workflow:

1. Define the role name (up to 16 alpha numeric characters)
2. Select the administration level (here: Cash or Currency Accounts)

3. Please select the appropriate company(ies) by moving from the Available to the Selected Companies box.
4. Existing accounts of the selected company(ies) will be listed. Select the appropriate accounts by moving from the Available to the Selected Companies box.
5. Select the appropriate products by moving from the Available to the Selected Companies box.
6. Click the Show Permissions button.
7. Tick-off the appropriate permissions.
   Note:
   - Verify Rights is optional and would force a verification after applying transaction orders before authorizing / approving for processing.
   - The 'Use' is used for the System Administration product.
8. Submit the data.

3.2.3.2 Maintain Authorization Rights

Below screen displays the existing permission of user role ‘New Auth Role’.

For example, line number 1 explains that for the certain account of company ‘Example Company, Inc.’ a Single Normal Limit (‘SNL’) of 1000 EUR, a Single Pre-approved Limit (‘SPL’) of 5000 EUR and a Joint Category (‘JC’) of 1 for Domestic Payments has been defined.

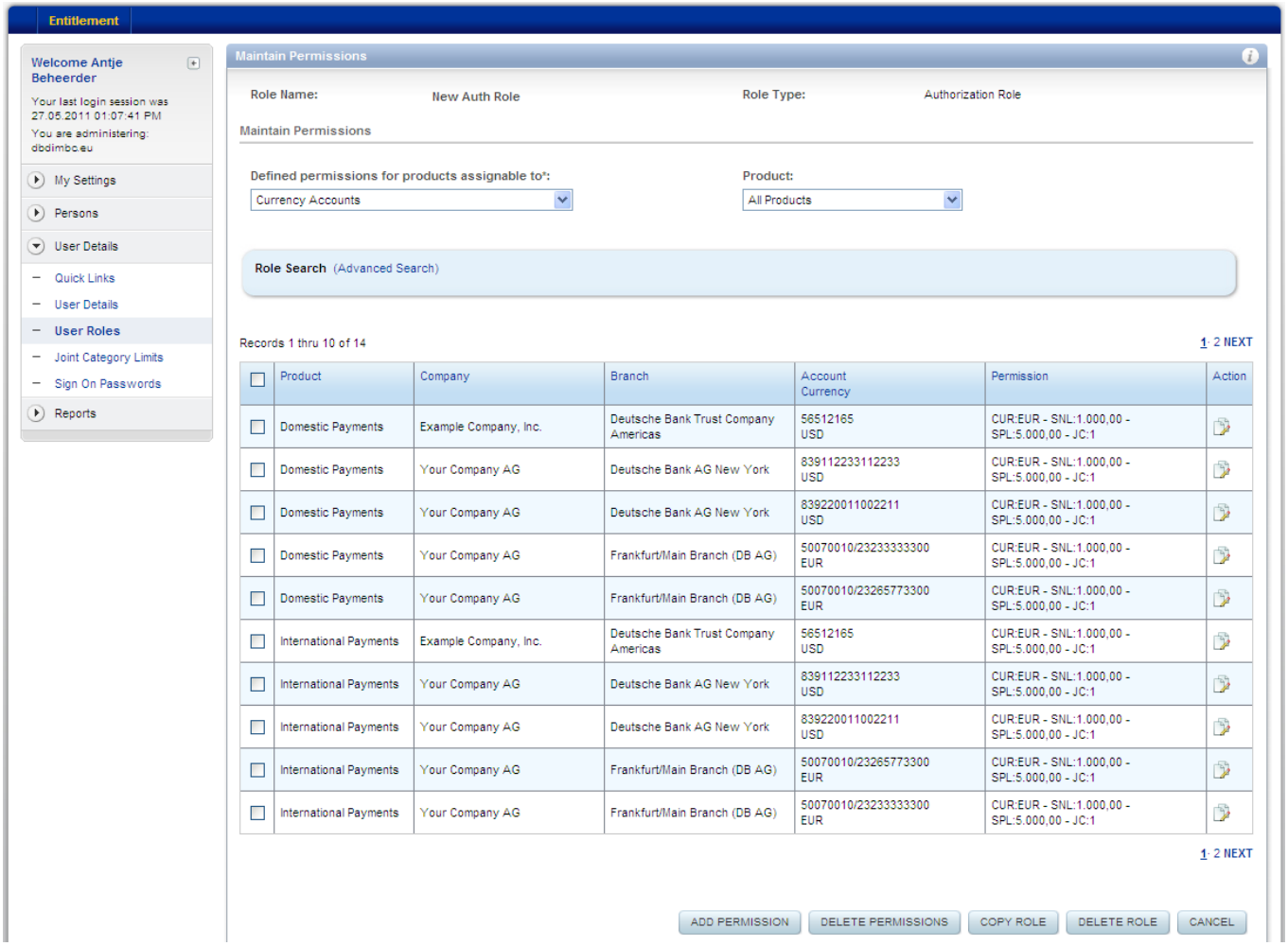
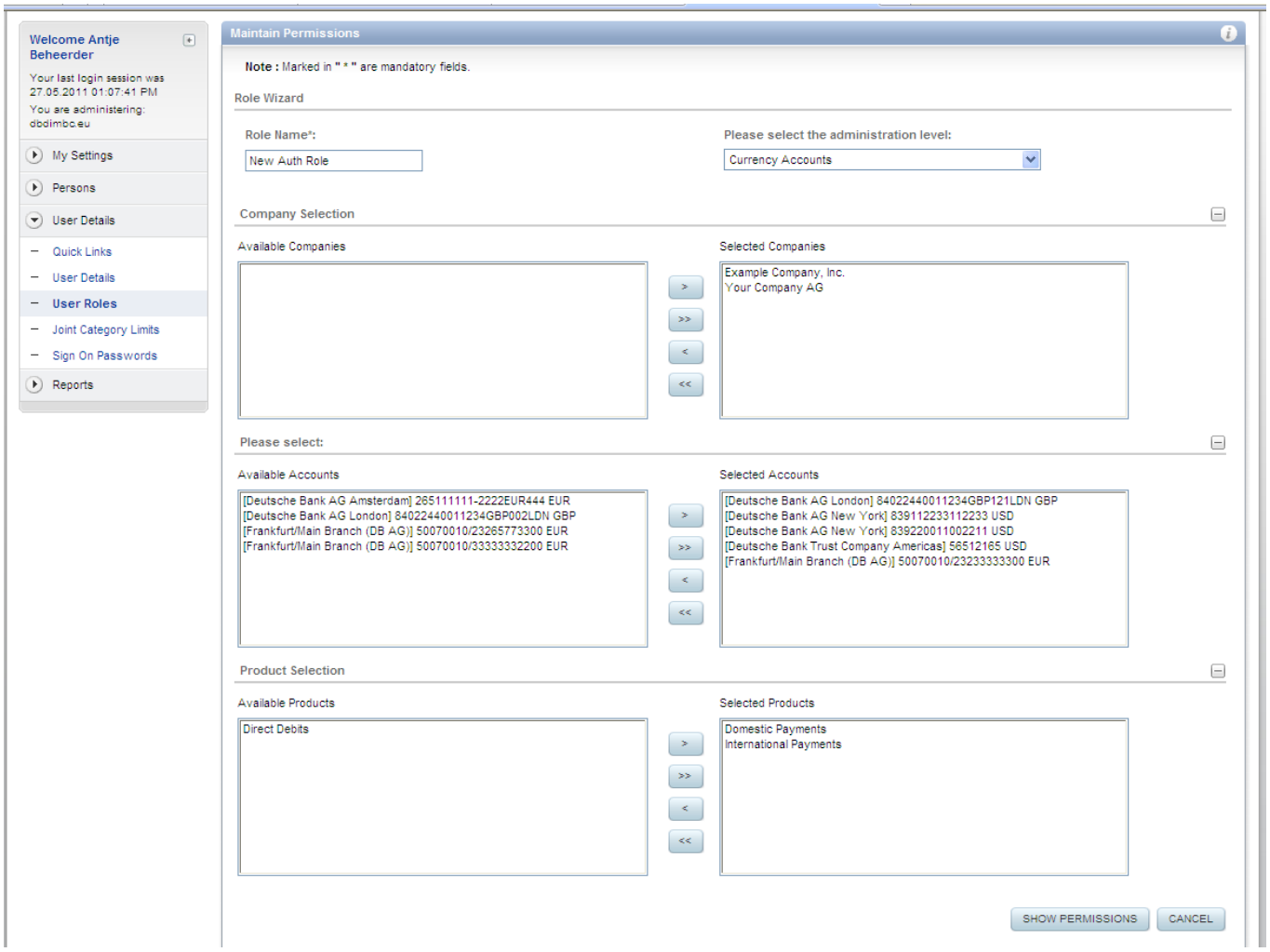

Entitlement
Welcome Antje Beheerder
Your last login session was 27.05.2011 01:07:41 PM
You are administering: dbdimbc.eu
My Settings
Persons
User Details
Quick Links
User Details
User Roles
Joint Category Limits
Sign On Passwords
Reports
Maintain Permissions
Role Name: New Auth Role
Role Type: Authorization Role
Maintain Permissions
Defined permissions for products assignable to*: Currency Accounts
Product: All Products
Role Search (Advanced Search)
Records 1 thru 10 of 14
1 2 NEXT
Product | Company | Branch | Account Currency | Permission | Action
Domestic Payments | Example Company, Inc. | Deutsche Bank Trust Company Americas | 56512165 USD | CUR:EUR - SNL:1.000,00 - SPL:5.000,00 - JC:1
Domestic Payments | Your Company AG | Deutsche Bank AG New York | 839112233112233 USD | CUR:EUR - SNL:1.000,00 - SPL:5.000,00 - JC:1
Domestic Payments | Your Company AG | Deutsche Bank AG New York | 839220011002211 USD | CUR:EUR - SNL:1.000,00 - SPL:5.000,00 - JC:1
Domestic Payments | Your Company AG | Frankfurt/Main Branch (DB AG) | 50070010/23233333300 EUR | CUR:EUR - SNL:1.000,00 - SPL:5.000,00 - JC:1
Domestic Payments | Your Company AG | Frankfurt/Main Branch (DB AG) | 50070010/23265773300 EUR | CUR:EUR - SNL:1.000,00 - SPL:5.000,00 - JC:1
International Payments | Example Company, Inc. | Deutsche Bank Trust Company Americas | 56512165 USD | CUR:EUR - SNL:1.000,00 - SPL:5.000,00 - JC:1
International Payments | Your Company AG | Deutsche Bank AG New York | 839112233112233 USD | CUR:EUR - SNL:1.000,00 - SPL:5.000,00 - JC:1
International Payments | Your Company AG | Deutsche Bank AG New York | 839220011002211 USD | CUR:EUR - SNL:1.000,00 - SPL:5.000,00 - JC:1
International Payments | Your Company AG | Frankfurt/Main Branch (DB AG) | 50070010/23265773300 EUR | CUR:EUR - SNL:1.000,00 - SPL:5.000,00 - JC:1
International Payments | Your Company AG | Frankfurt/Main Branch (DB AG) | 50070010/23233333300 EUR | CUR:EUR - SNL:1.000,00 - SPL:5.000,00 - JC:1
1 2 NEXT
ADD PERMISSION
DELETE PERMISSIONS
COPY ROLE
DELETE ROLE
CANCEL

Figure 21: Permissions summary of Maintain Authorization User Roles

Existing permissions can be removed by ticking the respective check box and pressing the “Delete Permissions” button, permissions can be amended by pressing the pencil icon in the Action column.

Please press the “Add Permission” button for applying new or further permissions.

The following Wizard (pop up window) will be displayed when adding a new Authorization role by clicking the Add Role bottom either in the Quicklinks or User Role screens:



Hit 'Show Permissions':

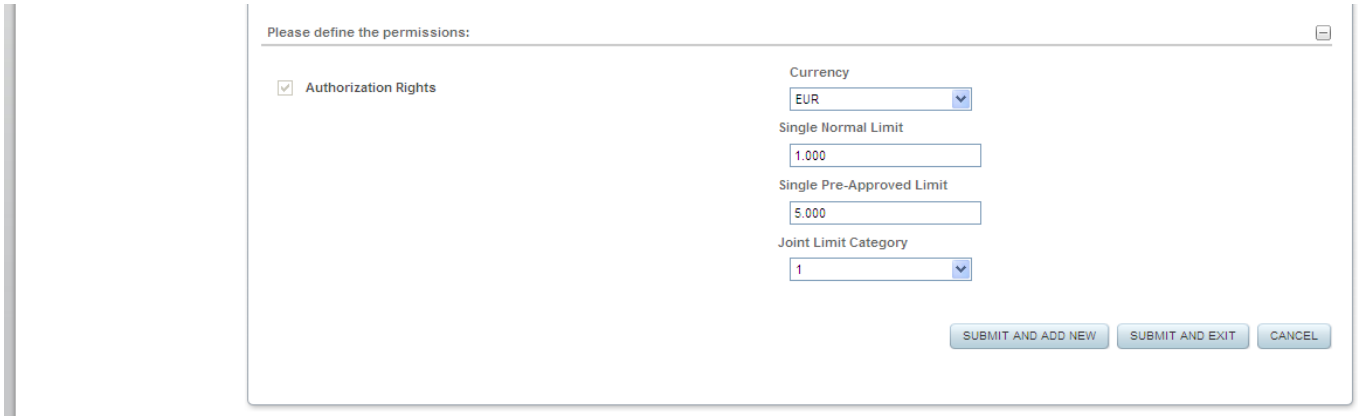


Figure 22: Wizard screen of Maintain Authorization User Roles

Administration workflow:

1. Define the role name (up to 16 alpha numeric characters)
2. Select the administration level (here: Cash or Currency Accounts)

3. Please select the appropriate company(ies) by moving from the Available to the Selected Companies box.
4. Existing accounts of the selected company(ies) will be listed. Select the appropriate accounts by moving from the Available to the Selected Companies box.
5. Select the appropriate products by moving from the Available to the Selected Companies box.
6. Click the Show Permissions button.
7. Define the (reference) currency, single limit amount, single pre-approved limit amount and joint category.
8. Submit the data.

Note:
When the Authorization Role is assigned to an Authorized Person (compare 3.1.2.4), a validation is been performed for certain DB accounts (depending on the account maintaining DB branch, please check with your Implementation Manager) to ensure that the Authorization rights defined via this Role are within the Authorized Person's Signatory Rights, as specified in the Company Mandate. This check will include validation of the Authorization Limits (Single Limits and Joint Limits)

3.2.3.3 Approving User Roles

Each operation is subject to an approval to be performed by a second Customer Self Administrator (dual control). The change will only be active after an approval.

In below example, the first line item is in Pending Approval status:

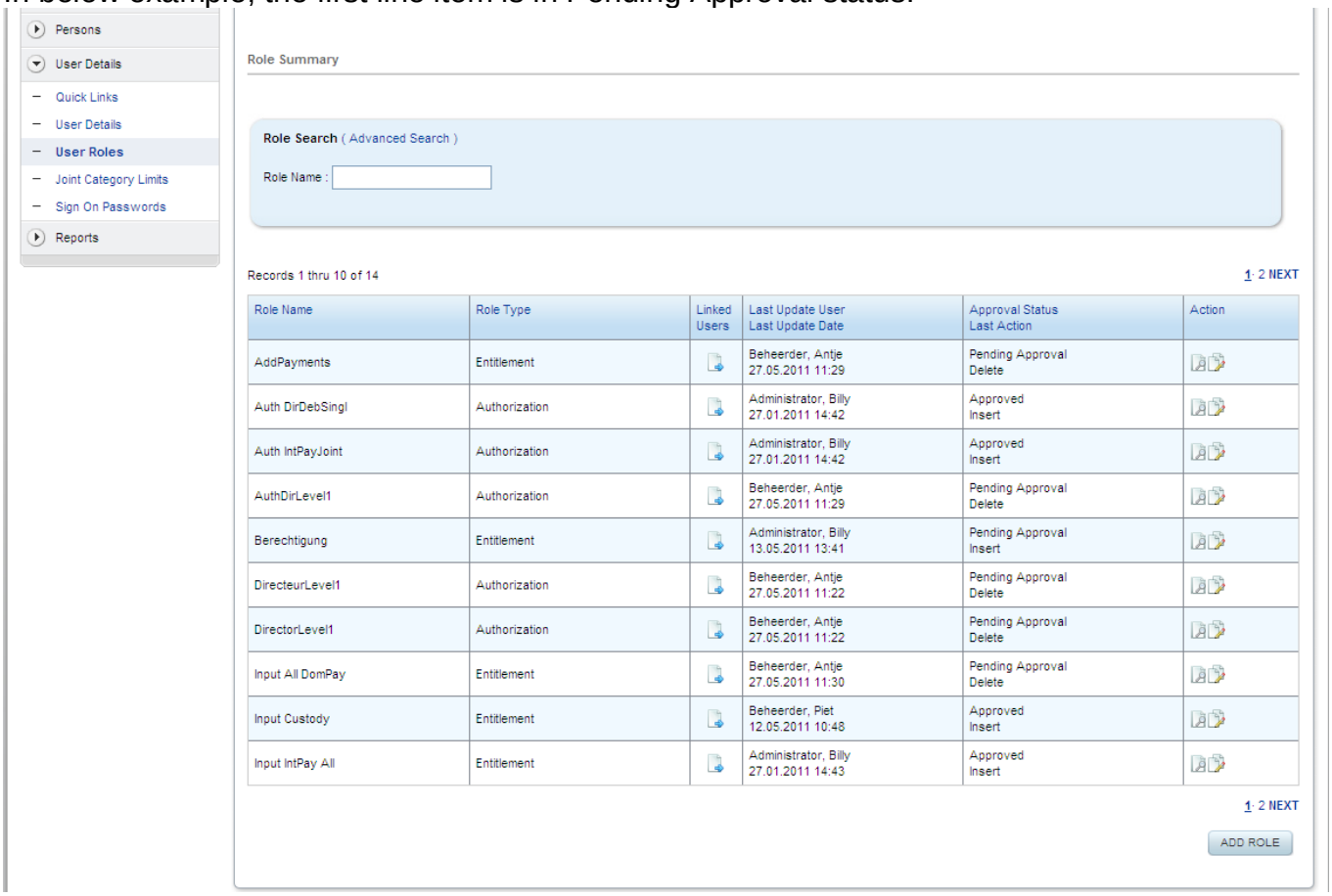

Persons
User Details
Quick Links
User Details
User Roles
Joint Category Limits
Sign On Passwords
Reports
Role Summary
Role Search (Advanced Search)
Role Name :
Records 1 thru 10 of 14
1 2 NEXT
Role Name | Role Type | Linked Users | Last Update User Last Update Date | Approval Status Last Action | Action
AddPayments | Entitlement | Beheerder, Antje 27.05.2011 11:29 | Pending Approval Delete
Auth DirDebSingl | Authorization | Administrator, Billy 27.01.2011 14:42 | Approved Insert
Auth IntPayJoint | Authorization | Administrator, Billy 27.01.2011 14:42 | Approved Insert
AuthDirLevel1 | Authorization | Beheerder, Antje 27.05.2011 11:29 | Pending Approval Delete
Berechtigung | Entitlement | Administrator, Billy 13.05.2011 13:41 | Pending Approval Insert
DirecteurLevel1 | Authorization | Beheerder, Antje 27.05.2011 11:22 | Pending Approval Delete
DirectorLevel1 | Authorization | Beheerder, Antje 27.05.2011 11:22 | Pending Approval Delete
Input All DomPay | Entitlement | Beheerder, Antje 27.05.2011 11:30 | Pending Approval Delete
Input Custody | Entitlement | Beheerder, Piet 12.05.2011 10:48 | Approved Insert
Input IntPay All | Entitlement | Administrator, Billy 27.01.2011 14:43 | Approved Insert
1 2 NEXT
ADD ROLE

Figure 23: User Role Summary where records is in 'pending approval' status

A second Customer Self Administrator needs to invoke the record (pressing the pencil icon) and can choose to Approve or Rollback it (there will be respective buttons in the bottom of the screen):

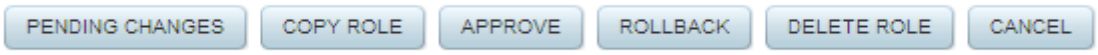


Figure 24: Approve & Rollback button

3.2.4 Maintain Joint Category Limits

A Joint Category Limit defines the payment amount that may be approved by 2 authorizers.

After clicking the 'Joint Category Limits' option, existing joint categories will be listed:

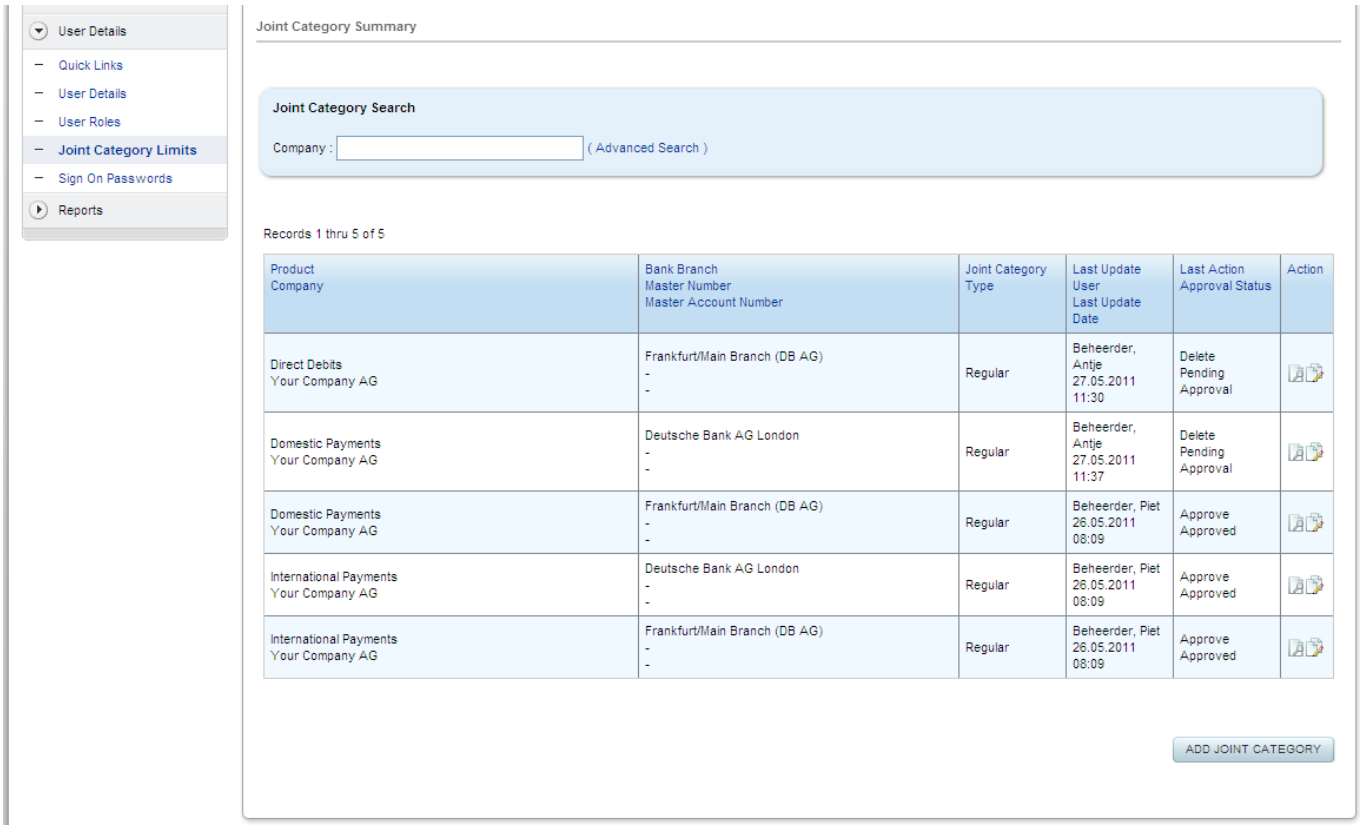


Figure 25: Joint Category Summary screen

One authorizer alone may approve an amount of up to 1.000 EUR, but with a second authorizer, they may approve between them, an amount of more than 1.000 EUR but with a limit of 5.000.000 EUR (example, see Figure 20).

Following screen depicts an example where for a company 'Example Company, Inc.' for accounts with DB Frankfurt and DB Amsterdam for the products Domestic and International Payments a joint limit of 5,000,000 EUR for category 1 has been setup.

The category 1 has to be defined accordingly in the authorization role (see Figure 20).

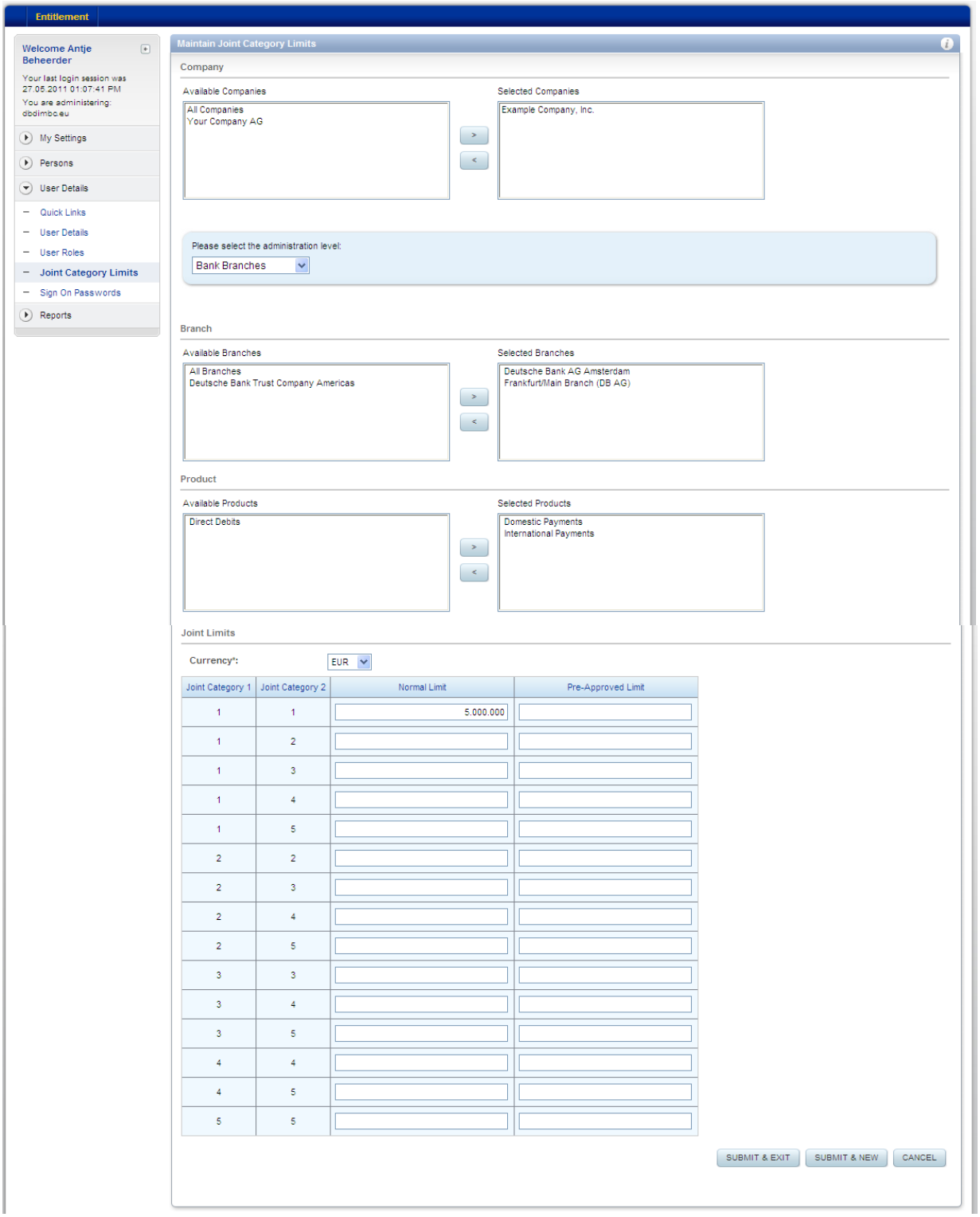


Figure 26: Maintain Joint Categories screen

3.2.5 Maintain Sign-On Passwords

Via this screen, the Customer Self Administrator is able to either create a db-direct internet logon password for a new user as well as reset of a password for an existing user, who might have forgotten his/ her password.

A created or reset password has to be approved by a second Customer Self Administrator (dual control), who needs to select the respective user from the drop down list. Users with pending approval status will be indicated via [U].

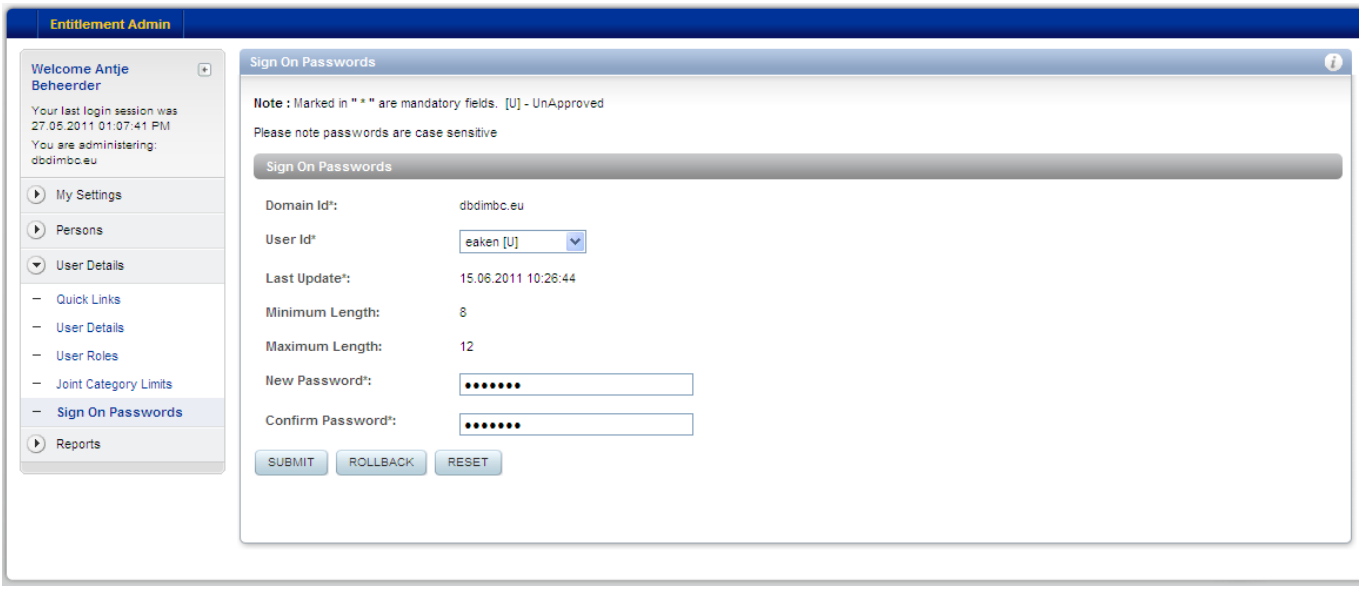


Figure 27: Sign On Password screen

Once controlled, the Customer Self Administrator can now communicate the password to the respective user (via phone, email, letter, etc.), who will be prompted to change the password with the first logon to db-direct internet.

Please note, that db-direct internet itself will, for security reasons, not distribute a message (like email).

3.3 Active User Reports

Reports on active user details, roles and joint category limits are available and can be generated by Customer Self Administrators.

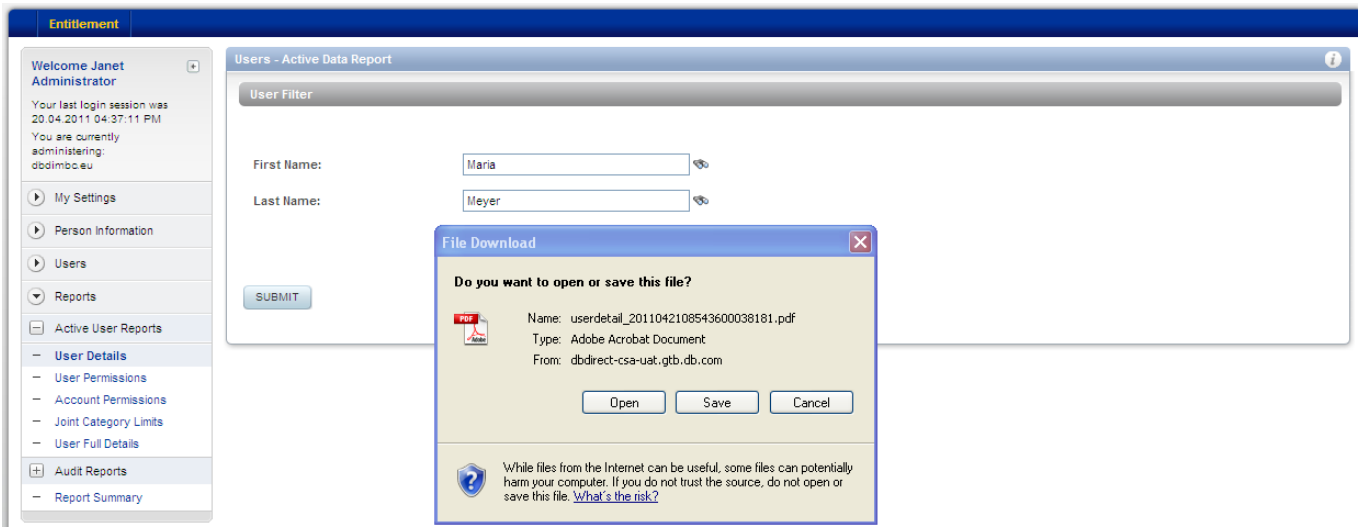


Figure 28: Request screen for generating an Active User Report

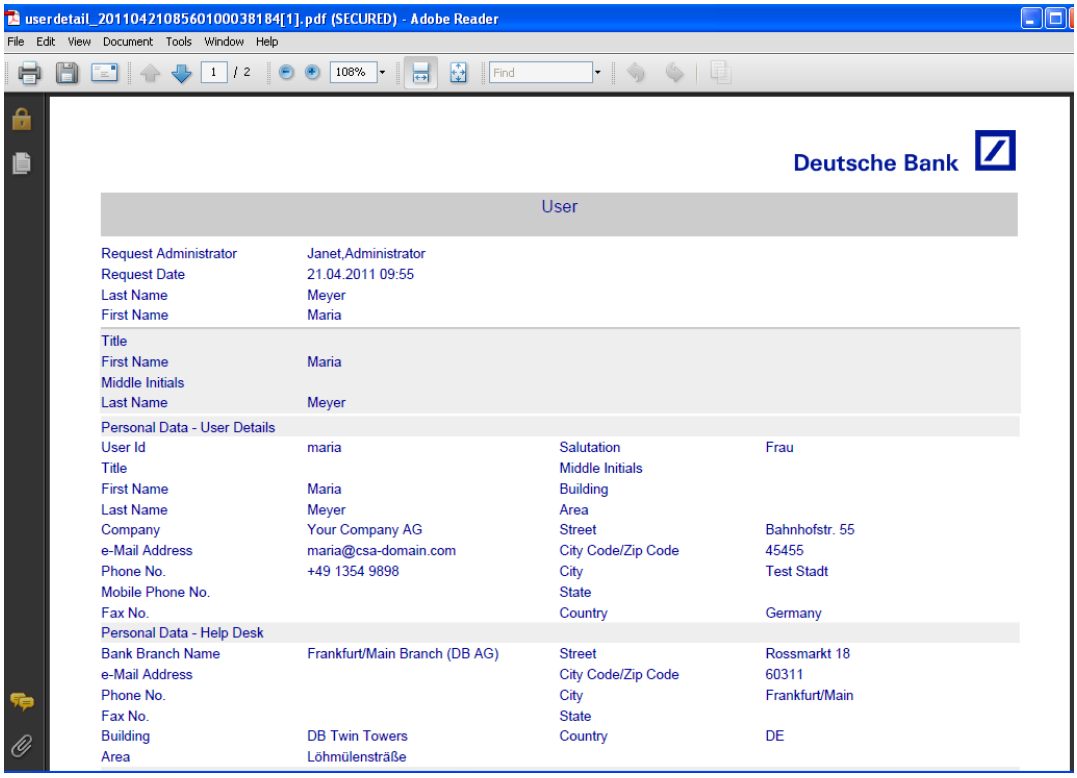


Figure 29: Active User Report example

3.4 Audit Reports

Audit reports on all user details, roles and joint category limits that have been maintained are available and can be generated by Customer Self Administrators.

In addition, other audit reports are available on: User Access Failures, Authorization Failures, User Access Audit Trails, Password Resets, Amended/Deleted Transactions, Deleted Files Audit Trail, ERP Import / Export Audit Trail and Beneficiary Audit Trails.

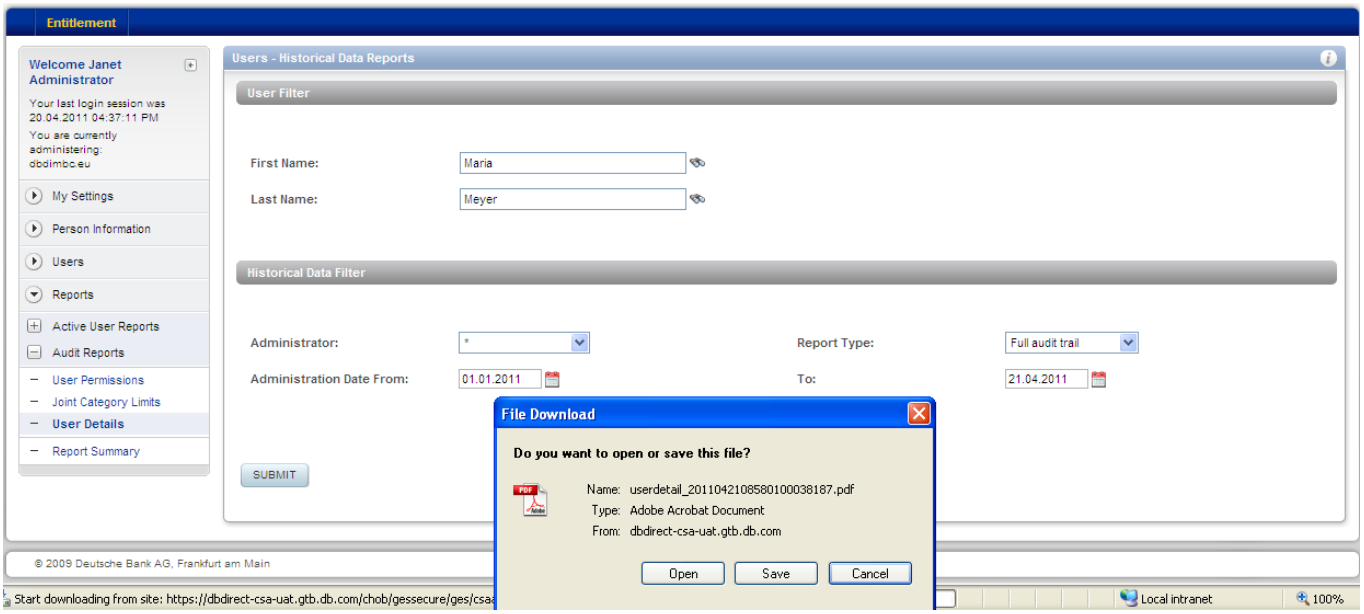


Figure 30: Request screen for generating a User Audit Report

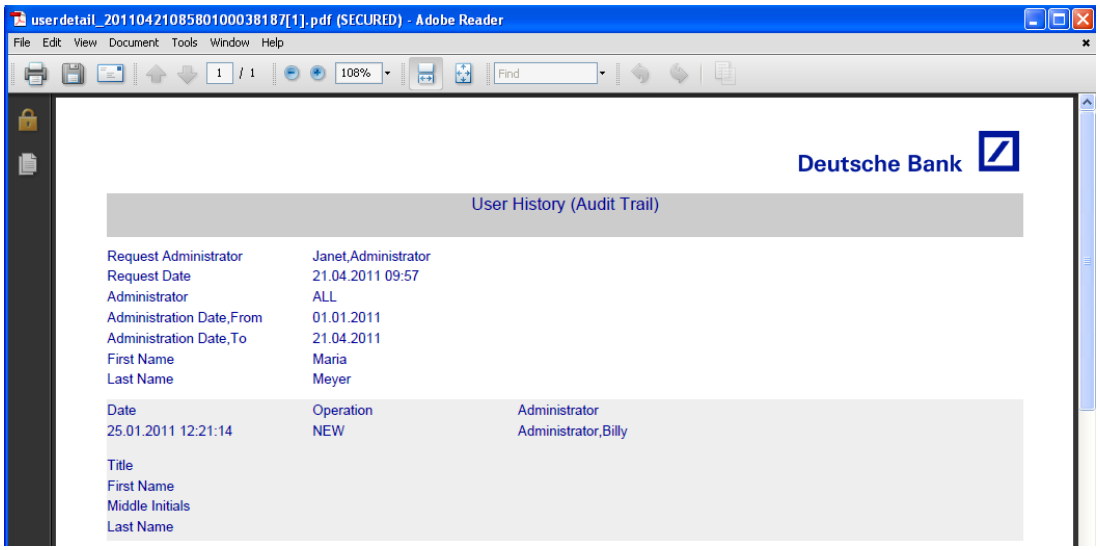


Figure 31: User Audit Report example

The Report Summary is listing reports that have been created:

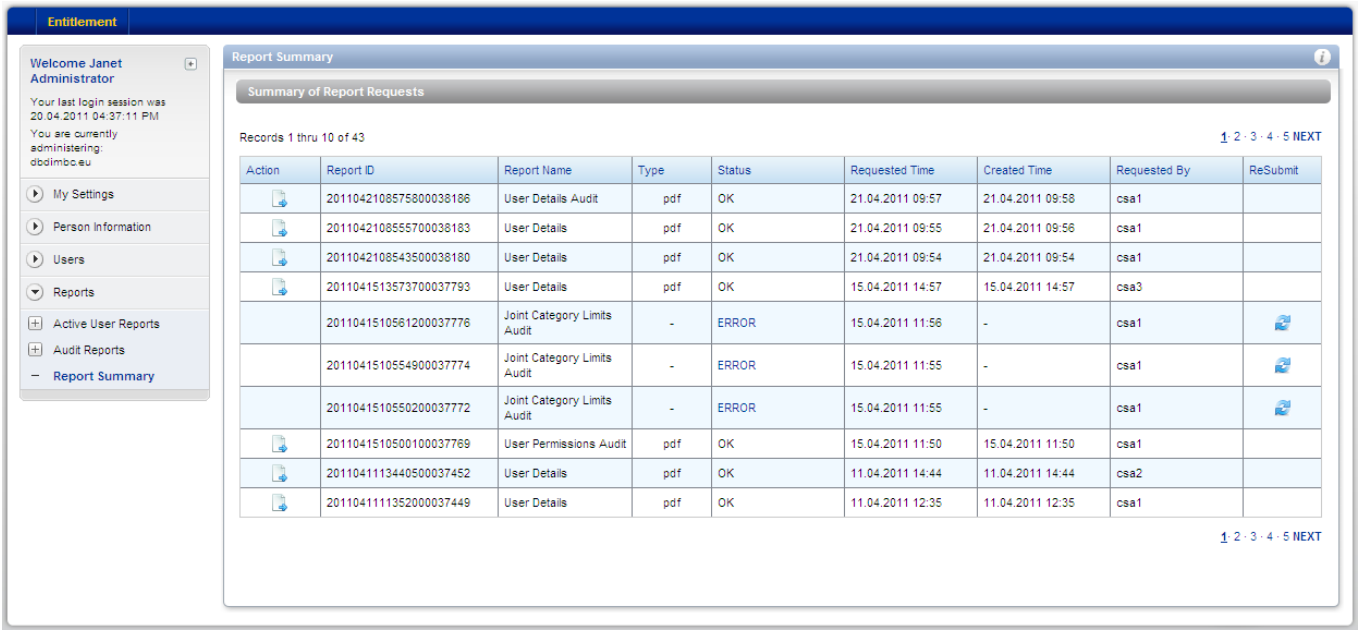

Entitlement
Welcome Janet Administrator
Your last login session was 20.04.2011 04:37:11 PM
You are currently administering: dbdimbc.eu
My Settings
Person Information
Users
Reports
Active User Reports
Audit Reports
Report Summary
Report Summary
Summary of Report Requests
Records 1 thru 10 of 43
1 · 2 · 3 · 4 · 5 NEXT
Action | Report ID | Report Name | Type | Status | Requested Time | Created Time | Requested By | ReSubmit
20110421085758000038186 | User Details Audit | pdf | OK | 21.04.2011 09:57 | 21.04.2011 09:58 | csa1
20110421085557000038183 | User Details | pdf | OK | 21.04.2011 09:55 | 21.04.2011 09:56 | csa1
20110421085435000038180 | User Details | pdf | OK | 21.04.2011 09:54 | 21.04.2011 09:54 | csa1
20110415135737000037793 | User Details | pdf | OK | 15.04.2011 14:57 | 15.04.2011 14:57 | csa3
20110415105612000037776 | Joint Category Limits Audit | - | ERROR | 15.04.2011 11:56 | - | csa1
20110415105549000037774 | Joint Category Limits Audit | - | ERROR | 15.04.2011 11:55 | - | csa1
20110415105502000037772 | Joint Category Limits Audit | - | ERROR | 15.04.2011 11:55 | - | csa1
20110415105001000037769 | User Permissions Audit | pdf | OK | 15.04.2011 11:50 | 15.04.2011 11:50 | csa1
20110411134405000037452 | User Details | pdf | OK | 11.04.2011 14:44 | 11.04.2011 14:44 | csa2
20110411113520000037449 | User Details | pdf | OK | 11.04.2011 12:35 | 11.04.2011 12:35 | csa1
1 · 2 · 3 · 4 · 5 NEXT

Figure 32: Report Summary example

4 Table of Figures

Figure 1: Access the CSA module from the main menu of the dbdi homepage 6
Figure 2: Quick Links screen 8
Figure 3: User summary from the User Details menu 9
Figure 4: Buttons displayed in case an object is "Pending Approval" 10
Figure 5: Objects with Last Update User as "CAAA, Import Approval" 10
Figure 6: Personal Data tab of User Details 11
Figure 7: Personal Data screen accessed via User Details 12
Figure 8: Maintain Person summary 13
Figure 9: Personal Data tab of Maintain Person 13
Figure 10: Authentication tab of the Maintain User screen 14
Figure 11: Entitlement Rights tab of the Maintain User screen 15
Figure 12: Authorization Rights tab Maintain Users screen 16
Figure 13: User Configuration of the Maintain User screen 17
Figure 14: Summary from the User Details menu, where one user records are in ‘pending approval’ status 18
Figure 15: Approve & Rollback button 19
Figure 16: User Lock flags 20
Figure 17: User Self Password reset via dbdi logon screen 20
Figure 16: Summary screen of Maintain User Roles 21
Figure 17: Permissions summary of Maintain Entitlement User Roles 22
Figure 18: Wizard screen of Maintain Entitlement User Roles 23
Figure 19: Permissions summary of Maintain Authorization User Roles 25
Figure 20: Wizard screen of Maintain Authorization User Roles 26
Figure 21: User Role Summary where records is in ‘pending approval’ status 28
Figure 22: Approve & Rollback button 28
Figure 25: Joint Category Summary screen 29
Figure 23: Maintain Joint Categories screen 30
Figure 24: Sign On Password screen 31
Figure 25: Request screen for generating an Active User Report 32
Figure 26: Active User Report example 32
Figure 27: Request screen for generating a User Audit Report 33
Figure 28: User Audit Report example 33
Figure 29: Report Summary example 34